555-7001-302

Meridian 1

Meridian Mail

System Administration Guide for Multi-Customer Systems

Product release 12 Standard 1.0 January 1998

NORTEL
NORTHERN TELECOM

Meridian 1

Meridian Mail
System Administration Guide for Multi-Customer Systems

Publication number:	555-7001-302
Product release:	12
Document release:	Standard 1.0
Date:	January 1998

© 1993, 1994, 1995, 1996, 1997, 1998 Northern Telecom
All rights reserved

Printed in the United States of America

Information is subject to change without notice. Northern Telecom reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Meridian 1, Meridian, and Nortel are trademarks of Northern Telecom.

Publication history

January 1998

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 12 base software.

November 1996

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 11 base software.

August 1995

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 10 base software.

April 1995

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 9.5 base software.

March 1994

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 9 base software.

April 1993

Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide for Multi-Customer Systems* is intended for Meridian Mail Release 8 base software.

Contents

1 About this guide 1-1

Overview 1-2
What this guide is about 1-3
Who should use this guide 1-4
Systems supported by this guide 1-5
Structure of this guide 1-6
Typographic conventions 1-11
Referenced documents 1-14

2 Navigating through system and customer administration 2-1

Overview 2-2

Section A: The administration menu hierarchy 2-3

Overview of Meridian Mail Multi-Customer 2-4
The system administration menu hierarchy 2-8
The customer administration menu hierarchy 2-9
The Main menu 2-10
The Customer Administration menu 2-11
User administration 2-12
General administration 2-13
Voice administration 2-16
Hardware administration 2-21
System status and maintenance 2-22
Operational measurements 2-25
Class of Service administration 2-28
Fax administration 2-29
Network administration 2-30
Hospitality administration 2-32

Section B: Understanding menus, screens, and keys 2-35

Overview 2-36
Keypad functions 2-38

Meridian Mail menus 2-39
Meridian Mail screens 2-42
Getting around in screens 2-44
Entering information in fields 2-45
Softkeys 2-51
Getting help 2-52
Error messages 2-53

Section C: Meridian Mail features and interfaces 2-55
The main administration terminal and multiple administration terminals (MATs) 2-56
Meridian Mail feature availability 2-58
Meridian Mail telset interfaces 2-60

3 Logging on 3-1
Overview 3-2
Types of consoles 3-3
Logon/Status screen 3-4
Setting the system administration password 3-6
Setting the customer administration password 3-8
Changing the system administration password 3-10
Changing the customer administration password 3-12
Recovering a system administration password 3-14
Recovering a customer administration password 3-15
Logging on from the main administration terminal 3-17
Logging on from a MAT 3-19
Logging on from a remote terminal (non-EC system) 3-21
Logging on from a remote terminal (EC system) 3-24
Using a single terminal to access the M1 and Meridian Mail 3-29

4 Setting up the system 4-1
Overview 4-2

Section A: Basic setup procedures 4-3
Overview 4-4
Changing the system administration password 4-5
Checking the hardware configuration 4-6
Checking the system status 4-7

Checking the Channel Allocation Table 4-8
Configuring general system options 4-9
Setting up dialing translations 4-10
Setting up restriction and permission lists. 4-11
Defining classes of service 4-12
Configuring operational measurement options 4-13
Configuring optional features and other services 4-14
Setting up system security 4-15
Backing up the system. 4-16

Section B: Setting up customers **4-17**
Overview 4-18
Changing the customer administration password 4-19
Adding customers to the system 4-20
Enabling features for each customer 4-21
Assigning classes of service to each customer 4-22
Setting the attendant DN for each customer 4-23
Customizing voice messaging options for each customer . 4-24
Customizing voice security options for each customer. . . . 4-25
Adding voice service DNs. 4-26
Adding users to customers 4-27
Creating distribution lists 4-28
Configuring optional features and other services 4-29
Backing up the system from the system administration level 4-30

Section C: Setting up optional features **4-31**
Overview 4-32
Setting up the Outcalling feature. 4-33
Setting up the Voice Menus feature 4-34
Setting up the Voice Forms feature. 4-35
Setting up the Fax on Demand feature 4-36
Setting up the Meridian Networking feature. 4-37
Setting up the AMIS Networking feature 4-38
Setting up the Virtual Node AMIS Networking feature . . . 4-39
Setting up the Enterprise Networking feature 4-40
Setting up the Hospitality feature 4-41
Setting up the Meridian Mail Reporter feature 4-42
Setting up the Meridian Mail AutoAdmin feature 4-43
Setting up the ACCESS feature 4-44

5 Customer administration 5-1

Overview 5-2
New installations 5-3
Adding customers 5-4
Provisioning customers 5-9
Finding, listing, and printing customers 5-11
Selecting a customer to view or modify 5-17
Deleting customers 5-22

6 Making voice recordings 6-1

Overview 6-2
Types of recordings 6-4
How Call Answering uses personal greetings and personal verifications 6-7
Voice recording tips 6-11

Section A: Making recordings 6-13

Overview 6-14
Logging in to Meridian Mail 6-15
Recording a call answering greeting 6-18
Recording personal greetings 6-24
Recording a personal verification 6-26
Recording a personal verification for a system distribution list 6-31
Identifying remote site names 6-34
Recording a personal verification for the broadcast mailbox 6-38
Recording and sending broadcast messages 6-41
Making Voice Services recordings 6-44

Section B: VMUIF recordings 6-47

Overview 6-48
VMUIF introductory tutorials and the VMUIF login greeting 6-49
Recording the VMUIF login greeting 6-52

7 Setting up Meridian Mail security 7-1

Overview 7-2

Section A: Telecommunication criminals and the problems they pose 7-3

Overview 7-4
Designing a security system 7-7
Ongoing security measures 7-8

Section B: Using Basic Access Restrictions features 7-9

Overview 7-10
Trunk Group Access Restrictions 7-11
Class of Service 7-13
TGAR/TARG and CLS interaction 7-17
Transfer feature on modems 7-19

Section C: Features that modify access restrictions 7-21

Overview 7-22
System Speed Call 7-23
Authorization Codes 7-24
Station Specific Authorization Codes 7-25
Forced Charge Account 7-27
Controlled Class of Service 7-29
Enhanced Controlled Class of Service 7-32
Flexible Feature Codes—Electronic Lock 7-33
Code Restriction 7-34
New Flexible Code Restriction 7-36

Section D: Controlling remote access to calling privilege 7-39

Overview 7-40
Call Forward All Calls 7-41
Call Forward External Deny 7-42
Call Forward to Trunk Access Code—DID Calls 7-43
Internal Call Forward 7-44
Flexible Feature Codes—Remote Call Forward 7-45
User Selectable Call Redirection 7-46

Section E: Controlling access through Least Cost Routing (BARS/NARS) 7-47

Overview 7-48
Supplemental Digit Recognition 7-50

Supplemental Digit Restriction 7-52
Network Class of Service—Facility Restriction Level 7-55
Network Speed Call 7-58
Network Authorization Code 7-60
Authorization Code Conditionally Last 7-61
Time-of-Day Routing 7-64
Routing Control 7-67
Incoming Trunk Group Exclusion 7-70

Section F: Controlling access to PBX administration programs 7-73
Overview 7-74
Password control 7-75
Limited access to overlays 7-77
Limited access password—user name 7-78
Single Terminal Access 7-79
Multi-user login 7-80
Input/Output port recovery 7-81
History file 7-82

Section G: Controlling Direct Inward System Access7-83
Overview 7-84
DISA and security codes 7-85
DISA and Class of Service 7-86
DISA and authorization codes 7-87

Section H: Restriction/Permission lists 7-89
Overview 7-90
What are restriction/permission lists and codes? 7-91
Defaults 7-93
Understanding how restriction/permission codes work . . . 7-94
Recommendations for using the first four restriction/permission lists 7-97
Defining and applying restriction/permission lists 7-99

Section I: Controlling access to Meridian Mail services and features 7-103
Overview 7-104
Custom Revert 7-106
Thru-Dial 7-109
Call Answering or Express Messaging 7-110
Extension dialing (mailbox thru-dial) 7-112

Fax on Demand 7-115
Remote Notification 7-116
Delivery to Non-User 7-118
External Call sender 7-120
AMIS Networking 7-121

Section J: Controlling access to Meridian Mail mailboxes 7-123
Overview 7-124
Using the Voice Security Options screen 7-125
Default security settings 7-131
Initial password change 7-133
Password display suppression 7-135
Password prefix 7-136
Password length 7-138
Forced regular password changes 7-139
Invalid logon attempts 7-142
Modifying mailbox security settings 7-146
Restricting off-site access to mailboxes 7-147
Disabling unused mailboxes 7-148

Section K: Monitoring access to Meridian Mail mailboxes and features 7-149
Overview 7-150
Hacker Monitor 7-151
Mailbox Login Monitoring 7-152
Thru-Dial Monitoring 7-154
CLID Monitoring 7-158
The Services Summary Traffic report 7-161

Section L: Equipment security 7-163
Overview 7-164
Switchroom access 7-165
Administration terminals 7-166
Meridian Mail and switch printouts 7-167

8 User administration—an overview 8-1

Section A: Introduction to User Administration 8-3
The User Administration menu 8-4
Types of users 8-6
Distribution lists 8-9

Limitations and guidelines 8-10
Support for multiple appearance DNs 8-11

Section B: New user planning 8-13
Overview 8-14
Class of service planning 8-15
Distributing local voice users evenly over volumes 8-17
Guidelines for adding users to a system that has disk shadowing 8-19
Guidelines for adding a large number of users 8-20
How user models in pre-Release 9 systems are converted to classes of service 8-21

9 Local voice users 9-1

Section A: Adding local voice users 9-3
Integrated mailbox administration 9-4
Before you begin adding local voice users 9-5
Adding a local voice user 9-7
Accessing the Add Local Voice User screen 9-9
The Add Local Voice User screen 9-12
Entering user information 9-14
Assigning a user to a class of service 9-17
Primary DN and extension DNs 9-21
The revert DN 9-23
The message waiting indication DN 9-27
Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN 9-29
Recording a personal verification for a user 9-32
Creating a remote notification schedule for a user 9-34
Setting other local voice user characteristics 9-37

Section B: Finding local voice users 9-43
Overview 9-44
Wildcard characters 9-45
Accessing the Find Local Voice Users screen 9-47
The Find Local Voice Users screen 9-48
Restrictions on how you can combine search criteria 9-65
Finding, listing, and printing local voice users 9-67
Reassigning a subset of local voice users to another class of service 9-71

Section C: Modifying and deleting local voice users 9-77
Accessing the View/Modify Local Voice User screen 9-78
Viewing and modifying a local voice user 9-82
Checking a user's status 9-84
Enabling a disabled mailbox 9-89
Changing a user's password 9-91
Monitoring mailbox logins for suspected hacker activity 9-92
Reassigning a mailbox to another user 9-94
Deleting a local voice user 9-95

10 Remote voice users 10-1

Section A: Introduction 10-3
What is a remote voice user?. 10-4
Remote voice user changes and enhancements. 10-6
Permanent remote voice users. 10-8
Temporary remote voice users 10-9

Section B: Adding remote voice users 10-11
The Add Remote Voice User screen. 10-12
Adding remote voice users through User Administration. 10-17
Recording a personal verification for a remote voice user. 10-19
Adding temporary remote voice users using RVU Propagation via Enterprise Networking. 10-21
Adding remote voice users using RVU Propagation via Bulk Provisioning 10-24

Section C: Finding remote voice users 10-27
Accessing the Find Remote Voice Users screen. 10-28
The Find Remote Voice Users screen. 10-29
Wildcard characters. 10-32
Finding, listing, and printing remote voice users 10-34

Section D: Modifying and deleting remote voice users 10-39
Viewing and modifying remote voice users 10-40
Manually deleting remote voice users. 10-45
How temporary remote voice users are automatically deleted from the system 10-49

11 Directory entry users 11-1

Overview 11-2
What is a directory entry user? 11-3
The Add Directory Entry User screen 11-4
Adding directory entry users 11-7
Recording a personal verification 11-8
The Find Directory Entry Users screen 11-10
Finding directory entry users 11-12
The List of Directory Entry Users screen 11-13
Printing directory entry users 11-15
Viewing or modifying directory entry users 11-16
Deleting directory entry users 11-18

12 Distribution lists 12-1

Overview 12-2
Understanding distribution lists 12-3
Limitations on distribution lists 12-4
Accessing the Distribution Lists softkeys screen 12-7
Adding a customer distribution list 12-9
Finding and viewing a customer distribution list 12-16
Modifying a customer distribution list 12-21
Printing a customer distribution list 12-23
Deleting a customer distribution list 12-25

13 General administration–an overview 13-1

General Administration 13-2

14 General options 14-1

Overview 14-2

Section A: Setting general options for the system 14-3

Accessing the General Options screen 14-4
Modifying the system name and system number 14-6
Defining the system addressing length and the supervised transfer delay 14-9
Setting the default customer number for IMA and ACCESS 14-12

Verifying installed features 14-14
Setting the date format for reports. 14-16
Setting printer port names 14-18

Section B: Setting general options for customers 14-21
Overview 14-22
Accessing the General Options screen at the customer administration level 14-23
Modifying the customer name and customer type 14-25
Enabling and disabling optional features for customers . . 14-27
Assigning classes of service to customers. 14-29
Setting the attendant DN 14-31

15 Volume administration 15-1
Overview 15-2
Volume names. 15-3
Volume contents 15-5
Volume distribution on single- and multi-node systems. . . 15-7
Voice storage capacity in single- and multi-node systems . 15-8
Checking volume capacity and usage levels for your system 15-10

16 Back up and restore Meridian Mail data 16-1
Overview 16-2

Section A: Preparing for backups 16-3
Overview 16-4
The three types of backups 16-5
Selective backup 16-6
Partial backup 16-8
Full backup 16-9
Volumes to back up. 16-10
How often to do backups. 16-11
Disk backup or tape backup 16-13
Before you perform a backup 16-14

Section B: Full and partial backups to tape 16-15
Overview 16-16
Performing a full backup to tape 16-18
Performing a partial backup to tape 16-20

Section C: Selective backup of users and services 16-23
Overview 16-24
Backing up all users 16-25
Backing up individual users 16-27
Backing up all users in a specified volume 16-29
Backing up all users assigned to a particular class of service 16-31
Backing up all users in a specific department 16-33
Backing up all multimedia services 16-35
Backing up selected individual multimedia services 16-37

Section D: Partial backups to disk 16-39
Performing a partial backup to disk 16-40

Section E: Scheduled backups 16-41
Scheduling the backup for a later time 16-42
Deleting a scheduled backup 16-45

Section F: Backup maintenance 16-47
Checking the status of a backup 16-48
Cleaning/maintaining the tape drive 16-52

Section G: Restoring information from a Selective backup 16-53
Overview 16-54
Restore from Selective backup 16-56

17 Password and system time changes 17-1
Overview 17-2
Changing the system administrator password 17-3
Changing the customer administrator password 17-5
Setting the minimum password length for all administrator passwords 17-7
The AdminPlus Download password 17-8
Changing the system time 17-10

18 Dialing translations 18-1

Overview 18-2

Section A: Introduction to dialing translations 18-3

Overview 18-4
Dialing translations 18-5
Default dialing prefixes and local system defaults 18-7
When default dialing translations defaults are required . . 18-10
Translation tables 18-12
When translation tables are required 18-14

Section B: How dialing translations work 18-17

Overview 18-18
How Meridian Mail collects digits 18-19
How dialing translations translate numbers 18-22
How Meridian Mail uses the dialable number 18-27

Section C: Setting up network dialing prefixes and local defaults 18-29

Overview 18-30
Worksheet for default dialing prefixes and local system defaults 18-31
Dialing translation defaults screen 18-33
Configuring the default dialing prefixes and local system defaults 18-37
Sample datafills for dialing translation defaults 18-40

Section D: Setting up translation tables 18-43

Overview 18-44
Identifying translation table requirements. 18-45
Identifying translation tables required on your system . . . 18-48
Local dialing to a different area/city code (area/city code required) 18-52
Local dialing to a different area/city code (no area/city code required). 18-56
Long distance dialing to the same area/city code (area/city code required) 18-59
Long distance dialing to the same area/city code (area/city code not required) 18-61
The View/Modify Translation Table screen 18-62
Configuring translation tables 18-64
Deleting translation tables 18-67

Section E: Sample datafills **18-69**
Overview 18-70
Datafill for countries without area/city codes 18-71
Datafill for a case where the switch handles dialing translation 18-72

Section F: Troubleshooting dialing translations **18-75**
Overview 18-76
Diagnosing and tracing problems in a dialing translation . 18-77

19 Routine maintenance 19-1
Overview 19-2
Monitoring Meridian Mail operation 19-3
Monitoring Meridian Mail hardware 19-5
Backing up the system 19-7
Cleaning the tape drive 19-9

20 Voice administration—an overview 20-1
Voice Administration 20-2

21 Voice messaging options 21-1

Section A: Introduction **21-3**
Overview 21-4
Accessing the Voice Messaging Options screen 21-5
The Voice Messaging Options screen 21-6
Defining voice messaging options 21-9

Section B: Languages on multilingual systems **21-11**
Overview 21-12
The default language and the user's preferred language . . 21-13
Setting up languages on systems without dual language prompting 21-15
Setting up languages on systems with dual language prompting 21-19

Section C: Customizing recordings **21-27**
Overview 21-28
Recording a customized call answering greeting 21-29

VMUIF introductory tutorials and the VMUIF login greeting. 21-32
Recording or disabling VMUIF tutorials and login greeting. 21-34

Section D: Defining operational characteristics for voice messaging 21-37
Overview 21-38
Enabling/disabling timed delivery and name dialing/ name addressing 21-40
Defining the lockout revert DN and personal distribution list prefix 21-45
Setting up the broadcast mailbox 21-47
Defining the billing DN. 21-51
Specifying the message delivery priority for networked systems 21-53
Specifying the mailbox full warning threshold 21-55
Specifying the maximum read message retention. 21-57
Enabling/disabling external call sender. 21-60
Enabling and configuring speed control 21-62

22 Display options 22-1
Overview 22-2
Different ways of sorting the VSDN table 22-3
Different ways of sorting the service definitions tables . . . 22-5
Different ways of sorting the Choice of Services and Menu Actions list 22-7
Changing the display options 22-9

23 Finding and printing VSDNs and service definitions 23-1
Overview 23-2
Wildcards 23-5
The Find Subset of VSDNs/Services screen 23-7
Finding and printing VSDNs. 23-9
Finding and printing service definitions 23-12

24 Configuring Meridian Mail services 24-1

Overview 24-2

Section A: Introduction 24-3

Automatic Call Distribution (ACD) 24-4
Meridian 1 – Meridian Mail connections 24-6
How Meridian Mail uses ACD 24-7
Types of queues. 24-9
Assigning DNs to services in the VSDN table 24-11

Section B: Planning your configuration 24-13

Overview 24-14
Types of Meridian Mail ports 24-15
Port requirements for Meridian Mail services. 24-18
Identifying the ports that are installed on your system . . . 24-20
Should you dedicate ports? 24-23
Dedicating ports because of mixed port types. 24-24
Dedicating ports to services 24-26
Dedicating ports to Meridian Mail customers. 24-28
Determining how many ACD queues you need 24-30
Determining how many dummy queues you need 24-31

Section C: Configuring the Meridian 1 for Meridian Mail services 24-33

Overview 24-34
Creating ACD queues for a totally shared configuration . 24-35
Creating ACD queues for a combination (shared and dedicated) configuration 24-37
Partially dedicating ports – blocking inbound calls only . 24-42
Partially dedicating ports – blocking outbound calls only 24-45
Fully dedicating ports – blocking inbound and outbound calls 24-51
Creating an agent queue 24-54
Adding agents to a queue 24-57
Creating a dummy queue. 24-61
Moving agents from one queue to another 24-63
Removing agents from a queue. 24-65
Modifying the Channel Allocation Table after moving agents 24-66

25 The VSDN table 25-1

Section A: Introduction 25-3
Overview 25-4
When to create a VSDN 25-5
Accessing the VSDN table 25-6
The VSDN table 25-9

Section B: Adding messaging VSDNs 25-11
Overview 25-12
Adding a VSDN for Voice Messaging 25-13
Adding a VSDN for Express Messaging. 25-15
Adding a VSDN for Call Answering 25-17
Adding a VSDN for hospitality voice messaging 25-19
Adding a VSDN for the Post-Checkout Mailbox service . 25-22
Adding a VSDN for the Greetings Service 25-24

Section C: Adding networking and ACCESS VSDNs 25-27
Overview 25-28
Adding a VSDN for AMIS Networking 25-29
Adding a VSDN for Meridian Networking. 25-31
Adding a VSDN for Enterprise Networking 25-33
Adding a VSDN for a Meridian ACCESS application . . . 25-36

Section D: Adding voice service and fax service DNs 25-39
Overview 25-40
Adding a VSDN for an announcement 25-41
Adding a VSDN for a thru-dial service. 25-43
Adding a VSDN for a voice menu 25-45
Adding a VSDN for a time-of-day controller 25-48
Adding a VSDN for Voice Prompt Maintenance 25-52
Adding a VSDN for Remote Activation 25-54
Adding a VSDN for a voice form 25-56
Adding a VSDN for the Transcription Service 25-58
Adding a VSDN for the Fax Information Service. 25-61
Adding a VSDN for the Fax Item Maintenance Service. . 25-64

Section E: Session profiles 25-67
What is a session profile? 25-68
How session profiles work when multiple services are invoked by one VSDN 25-70

How Meridian Mail 9/10 session profiles are converted to Meridian Mail 12 session profiles 25-72
Fax callback number formats 25-74
Determining how many VSDNs you need for a callback fax service 25-78
The basic service session profile 25-81
The full-service voice session profile 25-83
The full-service multimedia session profile 25-86
Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers 25-90
Specifying the channel capability, session time limit, and maximum number of invalid selections . . 25-92
Specifying fax service options 25-96
Specifying callback delivery options 25-102
Creating a custom cover sheet 25-107
Customizing the session profile for the Fax Item Maintenance Service 25-109

Section F: Viewing, modifying, and deleting VSDNs 25-115
Viewing and modifying a VSDN or session profile, or both 25-116
Deleting a VSDN 25-120

26 Voice services profile 26-1
Overview 26-2
Timeouts 26-3
How timeouts work 26-4
Modifying the voice services profile 26-6

27 Class of Service administration 27-1
Overview 27-2

Section A: Introduction to Class of Service 27-3
What is a Class of Service? 27-4
System Class of Service versus Personal Class of Service 27-6
How Class of Service is administered 27-7

Section B: Adding, changing, printing, and deleting System Classes of Service 27-9
Adding a Class of Service 27-10
The Add Class of Service screen (MMUI) 27-13
The Add Class of Service screen (VMUIF) 27-32
Assigning Classes of Service to customer groups. 27-51
The Find Class of Service screen 27-52
Finding, listing, or printing a Class of Service 27-54
Modifying a Class of Service 27-57
Deleting a Class of Service 27-62

Section C: Assigning Classes of Service to users 27-67
Assigning a Class of Service to a user 27-68
Creating and Assigning a Personal Class of Service to a user 27-69
The Class of Service conversion utility for converted systems 27-70

28 Hardware administration 28-1
Overview 28-2
The Hardware Administration menu. 28-3

Section A: Viewing the node configuration 28-5
Overview 28-6
The Node Configuration screen 28-7
The View Node screen 28-10

Section B: Viewing the data port configuration 28-17
Overview 28-18
The Data Port Configuration screen 28-23
Viewing data ports 28-25
View Terminal data ports 28-27
View Printer data port 28-30
View MMLink data port 28-32
View/Modify NWModem data port 28-34
View PMS data port 28-36
View AdminPlus data port 28-38
View Modem data port 28-40
View MSLink data port. 28-42

Section C: Printing node and data port information 28-45
Overview 28-46
Printing node and data port information 28-47

29 System status and maintenance 29-1
Overview 29-2
What is system status and maintenance? 29-3

Section A: System Status 29-5
Overview 29-6
The System Status screen 29-8
Disabling/activating the system (“Courtesy Down”) 29-15
Disabling/enabling nodes 29-17
Courtesy disabling/enabling ports 29-18

Section B: Card Status 29-19
Overview 29-20
The Card Status screen 29-21
Enabling/disabling cards 29-26
Running out-of-service diagnostics 29-27

Section C: DSP Port Status 29-29
Overview 29-30
The DSP Port Status screen 29-31
Detailed view of the DSP Port Status screen 29-38
Single mode and range mode 29-39
Disabling/enabling DSP ports in single mode 29-40
Disabling/enabling DSP ports in range mode 29-42

Section D: Channel Allocation Table 29-45
Overview 29-46
The Channel Allocation Table 29-47
Should you dedicate ports? 29-57
Modifying the Channel Allocation Table 29-60

Section E: Disk Maintenance 29-63
Overview 29-64
Checking disk status 29-65
Disabling disk shadowing (unsynching) 29-70
Replacing a failed disk 29-71
Reenabling disk shadowing (synching a disk pair) 29-72
Running diagnostics on a disk or a disk pair 29-74

Section F: Diagnostic Schedules 29-77
Overview 29-78
What are Voice Path Diagnostics? 29-79
Changing the parameters and schedule for diagnostics. . . 29-80
Analyzing the results of the diagnostics 29-84

30 SEERs and Meridian Mail Alarms 30-1
Overview 30-2

Section A: SEERs and Alarms 30-3
What is a SEER? 30-4
Retrieving SEERs 30-6
What is an alarm? 30-9
How to check alarm status 30-10
Silencing an alarm 30-12

Section B: Customizing SEER processing 30-15
Overview 30-16
Using SEER remapping 30-17
Using SEER throttling. 30-20
Using SEER escalation 30-23

Section C: Notification options for SEERs and alarms 30-27
Overview 30-28
Notification options for SEERs and alarms 30-29
Using SEER filtering. 30-31
Using SEER triggering 30-35
SEERs printing 30-38
Setting the SEER printer port name 30-40

31 Operational Measurements 31-1
Overview 31-2

Section A: Overview of Operational Measurements (OM) 31-3
Overview 31-4
What are Operational Measurements? 31-5
How Operational Measurements are useful 31-7

Section B: Setting up Operational Measurements 31-11
Overview 31-12
Using the Operational Measurements menu 31-13
Calculating disk space required for OM data storage 31-16
Operational Measurements Options screen 31-20
Fields in the Operational Measurement Options screen . . 31-22
Setting Meridian Mail to collect and receive data. 31-25

Section C: Interpreting Operational Measurements 31-27
Overview 31-28
Calculating centi-call seconds 31-29
Interpretation guidelines 31-30

32 Operational Measurements traffic reports 32-1
Overview 32-2

Section A: Generating traffic reports 32-3
Overview 32-4
Traffic Reports screen 32-5
Generating traffic reports 32-7

Section B: Traffic reports 32-9
Overview 32-11
Services Summary report 32-12
Fields in the Services Summary report 32-13
Analyzing the Services Summary report. 32-15
Voice Messaging Detail report 32-18
Fields in the Voice Messaging Detail report. 32-19
Analyzing the Voice Messaging Detail report 32-21
Channel Usage Detail report 32-22
Fields in the Channel Usage Detail report 32-23
Analyzing the Channel Usage Detail report 32-25
Services Detail report 32-26
Fields in the Services Detail report 32-27
Analyzing the Services Detail report. 32-29
Networking Detail report 32-31
Fields in the Networking Detail report 32-32
Analyzing the Networking Detail report. 32-35
AMIS Networking Detail report 32-37
Fields in the AMIS Networking Detail report. 32-38
Analyzing the AMIS Networking Detail report 32-40

Outcalling Detail report 32-41
Fields in the Outcalling Detail report 32-42
Analyzing the Outcalling Detail report 32-45
Fax Delivery Detail report 32-47
Fields in the Fax Delivery Detail report 32-48
Analyzing the Fax Delivery Detail report 32-50
Disk Usage Detail report 32-52
Fields in the Disk Usage Detail report 32-53
Analyzing the Disk Usage Detail report 32-54
Hospitality Statistics report 32-56
Fields in the Hospitality Statistics report 32-57
Analyzing the Hospitality Statistics report 32-58
Guest Console Statistics report 32-59
Fields in the Guest Console Statistics report 32-60
Analyzing the Guest Console Statistics report 32-61

33 User Usage reports 33-1

Overview 33-2
The User Usage Reports screen 33-3
Fields in the User Usage Reports screen 33-4
Generating User Usage reports 33-7
User Usage report 33-9
Fields in the User Usage report 33-11
Analyzing User Usage reports 33-14

34 Audit Trail reports 34-1

Overview 34-2

Section A: Collecting Audit Trail data 34-3

Overview 34-4
Enabling the collection of audit trail data 34-5

Section B: Outcalling Audit Trail reports 34-9

Overview 34-10
Generating an Outcalling Audit Trail report 34-11
The Summary Outcalling Audit Trail report 34-15
Fields in the Summary Outcalling Audit Trail report 34-16
Analyzing the Summary Outcalling Audit Trail report . . 34-18
The Detail Outcalling Audit Trail report 34-19

Fields in the Detail Outcalling Audit Trail report 34-20
Analyzing the Detail Outcalling Audit Trail report 34-28

Section C: Fax Audit Trail reports 34-29
Overview 34-30
The Fax Audit Trail Report screen 34-31
The Summary Fax Audit Trail report 34-35
Fields in the Summary Fax Audit Trail report screen 34-36
Analyzing the Summary Fax Audit Trail report 34-37
The Detail Fax Audit Trail report 34-38
Fields in the Detail Fax Audit Trail report screen. 34-39
Analyzing the Detail Fax Audit Trail report 34-43

35 Bulk provisioning 35-1
Overview 35-2

Section A: Introduction to bulk provisioning 35-3
Overview 35-4
What is bulk provisioning? 35-5
Using bulk provisioning 35-6

Section B: Working with bulk provisioning data sets 35-9
Overview 35-10
Assembling bulk provisioning data sets 35-11
Creating and modifying bulk provisioning data sets. 35-14
Viewing and printing bulk provisioning data sets. 35-21
Deleting bulk provisioning data sets 35-25

Section C: Transferring bulk provisioning data onto tape 35-27
Overview 35-28
Copying provisioning data sets onto tape 35-29

Section D: Provisioning data into a Meridian Mail system 35-33
Overview 35-34
Before you start 35-35
Provisioning data. 35-37
Viewing and printing data conflicts 35-43

A **Integrated Mailbox Administration** **A-1**

Overview A-2

Section A: Interaction between IMA and Meridian Mail **A-3**

Overview A-4
What is Integrated Mailbox Administration? A-5
IMA data translations A-6
Synchronizing IMA and Meridian Mail databases A-9
IMA and Meridian Mail processing differences and implementation issues A-10

Section B: System installation using VMBA **A-15**

Overview A-16
Installing at a new site without a preconfigured database on Meridian Mail or the Meridian 1 core A-17
Installing at a new site with sets and VMBs preconfigured on the Meridian 1 core but not on Meridian Mail A-18
Installing at an existing site with VMBs preconfigured on Meridian Mail but not the Meridian 1 core A-20

B **Meridian Mail AutoAdmin Utility** **B-1**

Overview B-2
Introduction B-3
Meridian Mail AutoAdmin installation B-5
AutoAdmin Configurator B-12
AutoAdmin Utility B-21
The AutoAdmin window B-25
Using Meridian Mail AutoAdmin B-34
Troubleshooting B-51

Index **Index-1**

List of Fields **Fields-1**

Chapter 1

About this guide

In this chapter

Overview	1-2
What this guide is about	1-3
Who should use this guide	1-4
Systems supported by this guide	1-5
Structure of this guide	1-6
Typographic conventions	1-11
Referenced documents	1-14

Overview

Introduction

This system administration guide provides the procedures and related information necessary to administer a Meridian Mail Release 12 system operating on a Meridian 1 platform. This guide includes the initial setup of your system, its daily operation, and its routine maintenance.

Before you begin

All your hardware, including the main administration terminal and optional printer, must already be installed.

What this guide is about

Introduction

This guide explains how to set up, operate, and maintain your Meridian Mail system.

Administrative tasks

This guide contains information and procedures for the following:

- setting up the initial system configuration (normally a once-only operation)
- logging on and navigating
- adding users and maintaining the user database
- making voice recordings, such as announcements and voice menus
- administering fax services on the system
- setting up system security
- backing up the system
- monitoring system status
- performing routine maintenance
- monitoring traffic reports and system usage reports
- troubleshooting
- configuring special features on your system

Where more detailed information is available in other manuals, this guide directs you to the appropriate resources.

Administration level

In multi-customer systems, some tasks may be exclusive to either the System Administration or the Customer Administration level. The Administration level header will indicate where those tasks apply in the menu hierarchy.

Task frequency

Some of these tasks must be performed every day. Others are carried out frequently, while some need to be done only occasionally.

These tasks are performed either through menu-driven screens at your administration terminal or through your telephone.

Who should use this guide

Introduction

This guide is intended for users who are responsible for setting up, operating, and maintaining the Meridian Mail system.

Guide users

There are two main groups of users who refer to this guide:

- The guide's primary users rely on this documentation to do their job.
- The guide's secondary users may need to refer to the documentation to do their jobs.

Examples of users

The following table identifies the primary and secondary users of this guide.

Users	Example
Primary users	• database administrators located at customer sites who perform all Meridian Mail administration tasks • technical support personnel
Secondary users	• installation and maintenance technicians • database administrators located at customer sites who perform only basic Meridian Mail administration tasks • sales engineers • trainers and courseware developers • technical application specialists

Systems supported by this guide

Introduction

This administration guide is common to the following hardware platforms:

- Meridian Mail Modular Option
- Meridian Mail Modular Option EC
- Meridian Mail Option 11

All of these platforms are connected to a Meridian 1/SL-1 switch using an AML/CSL link.

Supported systems

Some of the features documented in this guide may not be installed on your system.

In addition, because certain features are hardware dependent, it may not be possible for you to install them.

To determine whether you can install a particular feature on your system, see “Meridian Mail feature availability” on page 2-58.

Structure of this guide

Introduction

This guide is organized to reflect the hierarchical set of procedures accessible from the Main Menu. Most items that appear in the Main Menu have a corresponding chapter describing the administrative tasks and the screens and fields required to complete the tasks.

Contents of this guide

This guide contains the following chapters.

Chapter number and title	Description
Chapter 1: About this guide	Identifies the purpose, scope, audience, and structure of this guide. Sets out the typographic conventions used in the guide. Explains the guide's structure. Lists the publications referred to in this guide.
Chapter 2: Navigating through system administration	Provides an overview of the functional areas presented in the System Administration menu. Describes basic screen navigation tools and techniques. Introduces the two Meridian Mail Release 12 user interfaces. Lists the features available for each Meridian Mail hardware platform and user interface.
Chapter 3: Logging on	Describes how to log on to Meridian Mail. Describes how to log on to the Meridian 1 switch through a Meridian Mail administration terminal.
Chapter 4: Setting up the system	Refers users to procedures for checking the provisioning of Meridian Mail Release 12. Provides an overview of a complete basic setup of Meridian Mail Release 12, with cross-references to relevant information and procedures in other chapters and guides.
Chapter 5: Customer Administration	Describes how to add, find, list, modify, or delete customers on your system. Describes how you must have customers on a multi-customer system before you add users.
Chapter 6: Making voice recordings	Describes how to make voice recordings for use by Meridian Mail.

Chapter number and title	Description
Chapter 7: Setting up Meridian Mail security	Identifies the high-risk areas of a Meridian Mail system and the types of abuse that can occur. Lists the measures that can be taken to set up and monitor system security. Describes the use of security features to prevent unauthorized mailbox access. Describes measures to prevent the use of Meridian Mail features for unauthorized long distance calling. Suggests procedures to prevent unauthorized use of the administration terminal. Describes the reporting features available to help administrators detect abuse.
Chapter 8: User administration — an overview	Introduces the concepts and issues concerning user administration. Cross-references appropriate chapters for routine user administration tasks of particular interest or concern.
Chapter 9: Local voice users	Describes procedures for administering local voice users.
Chapter 10: Remote voice users	Describes procedures for administering remote voice users.
Chapter 11: Directory entry users	Describes procedures for administering directory entry users.
Chapter 12: Distribution lists	Describes procedures for administering system distribution lists.
Chapter 13: General administration — an overview	Introduces the concepts and issues concerning general administration. Directs users to the appropriate chapters for routine general administration tasks.
Chapter 14: General options	Describes how to perform the tasks and locate the information available under the General Options screen.
Chapter 15: Volume administration	Describes the tasks that can be performed through the volume administration side of Volume and selective backups.

Chapter number and title	Description
Chapter 16: Back up and restore Meridian Mail data	Explains the importance of Meridian Mail system backups. Suggests which volumes to back up, and how frequently. Describes the two available backup media and how to perform a backup with either one. Describes the procedures for scheduling a backup to occur automatically at a later time and for checking on the status of a backup in progress.
Chapter 17: Password and system time changes	Describes how and how often to change the administration password and the AdminPlus password. Describes how to change Meridian Mail's system time setting.
Chapter 18: Dialing translations	Introduces the concept of dialing translations. Specifies the situations and features requiring dialing translations. Guides users through setting up dialing prefixes and translation tables appropriate to their system. Provides in-depth detail for those who wish to customize dialing translations.
Chapter 19: Routine maintenance	Lists the routine maintenance tasks recommended for optimum Meridian Mail operation.
Chapter 20: Voice administration—an overview	Provides an overview of voice administration. Describes the Voice Administration menu and its menu options. Directs users to the appropriate chapters for documentation of the menus and screens accessible from the Voice Administration menu.
Chapter 21: Voice messaging options	Describes the tasks that can be performed using the Voice Messaging Options screen.
Chapter 22: Display options	Describes how to change the display options for the Voice Services Administration screen using the Set Display Options screen.
Chapter 23: Finding and printing VSDNs and service definitions	Describes how to use the Find function to find and print VSDNs and service definitions.
Chapter 24: Configuring Meridian Mail services	Provides an overview of the configuration of Meridian Mail services: the setup of the Meridian 1 switch and Meridian Mail setup.

Chapter number and title	Description
Chapter 25: The VSDN table	Documents the procedures for configuring VSDNs for each Meridian Mail feature that potentially requires a DN.
Chapter 26: Voice services profile	Documents the tasks that can be performed using the Voice Services Profile screen. Provides information about the different kinds of timeouts and how they work.
Chapter 27: Class of Service administration	Introduces the concept of Class of Service and the types of Class of Service. Guides users through creating, assigning, changing, and deleting individual Classes of Service.
Chapter 28: Hardware administration	Describes the methods for viewing and printing out the configuration of Meridian Mail's dedicated nodes and data ports.
Chapter 29: System status and maintenance	Describes procedures for checking on system, card, and port status. Describes procedures for enabling and disabling certain system components as part of routine maintenance, troubleshooting, and replacement. Describes the use of the Channel Allocation Table during system expansion or reorganization.
Chapter 30: SEERs and Meridian Mail Alarms	Introduces the concepts of SEERs and Meridian Mail alarms. Describes how to customize a system's SEER processing protocols to control how certain SEER messages are categorized and reported.
Chapter 31: Operational Measurements	Provides an overview of the Operational Measurements feature and how it can be used to monitor Meridian Mail system activity. Describes how to generate, view, print, and analyze Operational Measurement reports.
Chapter 32: Operational Measurements traffic reports	Provides information and procedures for Operational Measurements traffic reports.
Chapter 33: User Usage reports	Provides information and procedures for Operational Measurements user usage reports.
Chapter 34: Audit Trail reports	Provides information and procedures for Operational Measurements audit trail reports.

Chapter number and title	Description
Chapter 35: Bulk provisioning	Introduces the concept of bulk provisioning. Offers examples of situations where bulk provisioning can be used. Describes procedures for transferring bulk provisioning data onto tape and into another Meridian Mail system.
Appendix A: Integrated Mailbox Administration	Presents information and procedures for avoiding data corruption or task conflicts when using the Integrated Mailbox Administration feature to administer mailboxes.
Appendix B: Meridian Mail AutoAdmin Utility	Presents information and procedures for using Meridian Mail AutoAdmin to administer mailboxes from a PC, and to use data files from other applications to supply user information for new mailboxes.

Typographic conventions

Introduction

This topic describes the typographic conventions used in this guide for the following:

- softkeys
- keyboard keys or hardkeys
- telephone keypad keys
- text input
- fields in a menu
- values in a field
- system responses
- spoken words
- recorded prompts

Conventions

The following table identifies, describes, and provides examples of the conventions used in this guide.

Convention for	Description	Example
softkey	Softkeys are displayed on the administration menus and screens. They indicate which keyboard function keys you press to carry out specific Meridian Mail tasks. A softkey is referred to by its label (as displayed in the menu or screen) enclosed in square brackets. It appears in the same typeface as the accompanying text.	[Exit] [Record]
keyboard key or hardkey	A keyboard key or hardkey is referred to by its label enclosed in angle brackets. When two key names appear together, you press them both at the same time. A keyboard key or hardkey appears in the same typeface as the accompanying text.	<1> <Prev Screen> <Help> <Return> <Ctrl> <r>

Convention for	Description	Example
telephone keypad key	The telephone keypad keys that you press appear in bold print in the same typeface as the accompanying text.	Press **829** on the telephone keypad.
text input	Text that you type appears in bold print. In a procedure, it appears in the same typeface as the accompanying text. In other text, it appears in a different typeface from the accompanying text.	Type **m.**
fields in a menu	The name of a field is capitalized and appears in the same typeface as the accompanying text.	the Last Name field the Invalid Logon Attempt field
values in a field	A value in a field is capitalized and appears in the same typeface as the accompanying text.	The default is No.
system responses	System responses appear in the same typeface as the accompanying text. They are often introduced with **Result:.**	**Result:** The system prompts you for a password.
spoken words	The suggested wording of a greeting or an announcement appears in italics enclosed in double quotation marks.	You might want to include the following statement in your voice menu: "*Please wait on the line. An Attendant will be with you shortly.*"
recorded prompts	Prompts played by the system appear in italics enclosed in double quotation marks (the same as spoken words).	"*You have no new voice messages. One old message is still unsent.*"

Cross-references

For a cross-reference to another part of this guide or to another manual, the following conventions are used.

Cross-reference	Convention	Example
to another topic in this guide	This cross-reference is enclosed in double quotation marks.	For more information, see "Logging in to Meridian Mail" on page 6-15.
to another manual	The title of the manual appears in italics. The applicable reference number is also presented.	Refer to the *Meridian Mail System Installation and Modification Guide* (NTP 555-7001-215).

Referenced documents

Introduction

You may find it useful to have a number of additional resources available as you are reading this manual.

Referenced documents

The following table identifies the documents that are referred to in this guide.

Note: An "x" in a Nortel (Northern Telecom) Publication (NTP) number indicates that this digit varies, depending on the Meridian Mail hardware platform:

- 7041 indicates Meridian Mail Modular Option
- 7061 indicates Meridian Mail Modular Option EC
- 7071 indicates Option 11

NTP number	Title	Description
555-7001-000	*NTP Contents Overview*	Lists the NTPs in the Meridian Mail suite and provides a brief description of their content.
555-7001-100	*Meridian Mail Messaging Overview*	Provides an overview of the Meridian Mail system and features.
555-70x1-200	*Meridian Mail Site Installation and Planning Guide*	Documents the steps necessary to engineer and plan a Meridian Mail system. This is available only for Meridian Mail Modular Option and Modular Option EC.
555-7001-215	*Meridian Mail System Installation and Modification Guide*	Documents software installation, port reconfiguration, and upgrades, among other topics.
555-7001-221	*Hospitality Voice Services Implementation Guide*	Documents the implementation of a hospitality system.
555-70x1-250	*Meridian Mail Installation and Maintenance Guide*	Documents the installation of Meridian Mail hardware. Also describes how to provision the Meridian 1 switch for Meridian Mail.

NTP number	Title	Description
555-7071-210	*Meridian Mail Installation and Maintenance Guide* (Card Option)	Documents the installation of Meridian Mail hardware.
555-7001-241	*Meridian Networking Planning Guide*	Provides descriptive information and instructions for choosing a networking service.
555-7001-242	*AMIS Networking Installation and Administration Guide*	Documents the implementation of AMIS Networking (networking with the AMIS protocol).
555-7001-244	*Meridian Networking Installation and Administration Guide*	Documents the implementation of Meridian Networking (networking with modems).
555-7001-245	*Virtual Node AMIS Installation and Administration Guide*	Documents the implementation of Virtual Node AMIS Networking (a combination of Meridian Networking and AMIS Networking).
555-7001-246	*Meridian Mail Enterprise Networking Installation and Administration Guide*	Documents the implementation of Meridian Mail Enterprise Networking (networking without modems).
555-7001-305	*Meridian Mail System Administration Tools*	Documents additional administrative tools and utilities that are available at the tools level.
555-7001-310	*Meridian Mail Reporter System Administration Guide*	Documents the Meridian Mail Reporter feature, which allows you to use a PC to download information from the Meridian Mail system.
555-7001-315	*Meridian ACCESS Configuration Guide*	Documents the Meridian Mail and PBX configuration required to support Meridian ACCESS.
555-7001-316	*Meridian ACCESS Developer's Guide*	Documents how to develop and maintain Meridian ACCESS applications.
555-7001-318	*Meridian ACCESS Voice Prompt Editor User's Guide*	Documents how to use the voice prompt editor to create and maintain voice segment files and individual voice segments.

NTP number	Title	Description
555-7001-320	*Meridian Mail Outcalling Application Guide*	Documents the implementation of the Remote Notification feature and Delivery to Non-User feature.
555-7001-325	*Meridian Mail Voice Services Application Guide*	Documents the planning, configuration, and implementation of voice services.
555-7001-327	*Meridian Mail Fax on Demand Application Guide*	Documents the planning, configuration, and implementation of the fax information service and fax item maintenance service.
555-7001-510	*Meridian Mail Maintenance Messages (SEERs)*	Lists System Event and Error Reports (SEERs) to help isolate and fix system problems.
553-3001-300	*Meridian 1 X11 System Management Overview, Applications, and Security*	Provides an introduction to the system management facilities provided with the Meridian 1 switch.

Chapter 2

Navigating through system and customer administration

In this chapter

Overview	2-2
Section A: The administration menu hierarchy	2-3
Section B: Understanding menus, screens, and keys	2-35
Section C: Meridian Mail features and interfaces	2-55

Overview

Introduction

This chapter contains the following information:

- an overview of the multi-customer feature which creates two levels of administration
- an overview of how the menus are arranged into hierarchies at the system and customer administration levels
- an overview of the functional areas presented in the Main menu and the Customer Administration menu
- the layout of screens and menus
- navigation tools and techniques
- instructions on how to modify fields
- a list of the features available for each Meridian Mail hardware platform
- an introduction to the two Meridian Mail telset interfaces and the features available in each
  - Meridian Mail User Interface (MMUI)
  - Voice Messaging User Interface Forum (VMUIF)

Section A: The administration menu hierarchy

In this section

Overview of Meridian Mail Multi-Customer	2-4
The system administration menu hierarchy	2-8
The customer administration menu hierarchy	2-9
The Main menu	2-10
The Customer Administration menu	2-11
User administration	2-12
General administration	2-13
Voice administration	2-16
Hardware administration	2-21
System status and maintenance	2-22
Operational measurements	2-25
Class of Service administration	2-28
Fax administration	2-29
Network administration	2-30
Hospitality administration	2-32

Overview of Meridian Mail Multi-Customer

Description

The Meridian Mail Multi-Customer feature allows you to partition your Meridian Mail system in order to support a number of different user groups.

A user group is known as a *customer* in Meridian Mail.

Maximum number of customers

A single Meridian Mail system can support up to 2000 customers.

Benefits

By dividing your system into a number of customers, you can

- provide only the features that a particular customer needs
- configure features differently for different customers
- configure voice messaging differently for different customers
- enable the most appropriate telset interface (MMUI or VMUIF)
- bill customers separately based on the features and capabilities that are provided
- track how users in each customer are using the system and its features

Impact on administration

In a multi-customer system, there are two levels of administration:

- system administration
- customer administration

System versus customer administration

Some screens are available at one level of administration only. Other screens are available at both levels, but typically different fields are available to be modified at the different levels.

Screens and fields that are modified at the system administration level affect the entire Meridian Mail system. Screens and fields modified at the customer administration level apply to one customer only, the selected customer.

Tenants versus customers on the Meridian 1

On the Meridian 1, there are two distinct features: Multi-Customer and Multi-Tenant.

Multi-Customer on the Meridian 1 allows the PBX to be divided into a number of customers. If the Multi-Tenant feature is installed, these customers can be further subdivided into tenants.

All the tenants that belong to a particular customer share the same numbering plan and features as the customer. However, customers can have different numbering plans and features.

Multi-Customer on Meridian Mail

The Meridian Mail Multi-Customer feature supports the Meridian 1 Multi-Tenant feature, not the Multi-Customer feature.

If you are familiar with the Meridian 1, keep in mind that, in Meridian Mail, a customer is the equivalent to a Meridian 1 tenant.

Internal versus external callers

In a multi-customer system, only users within the same customer are considered internal users. Users on the same Meridian Mail system, but in other customers, are considered external.

Controlling external calls and messages

There are a number of fields that control communications with external callers.

Field	Screen	Description
Receive external messages	Add or View/ Modify Class of Service	This field determines whether users in a customer can receive messages from users in other customers. The default is Yes.
Send messages to external users	Add or View/ Modify Class of Service	This field determines whether users in a customer can send voice messages to users in other customers. The default is No.
External call-sender allowed	Voice Messaging Options	This field determines whether users in a customer can use the call sender feature to call back users in other customers or callers that are not on-switch. The default is No.

AMIS open network messages

If AMIS networking is installed, classes of service must be configured in a certain way if you want users in different customers to be able to send and receive AMIS open network messages.

The following fields must be set to Yes for both (sending and receiving) customers. These fields are in the Add and View/ Modify Class of Service screens:

- Receive AMIS Open Network Messages
- Compose/Send AMIS Open Network Messages

Limitations

The following are the limitations of the Multi-Customer feature:

- If Meridian Networking is installed, it can be enabled for one customer only.
- If Hospitality Voice Messaging is installed, it can be enabled for one customer only.

- If more than one language is installed on the system, you cannot selectively enable different languages for different customers. All installed languages are available to all customers.l

CAUTION

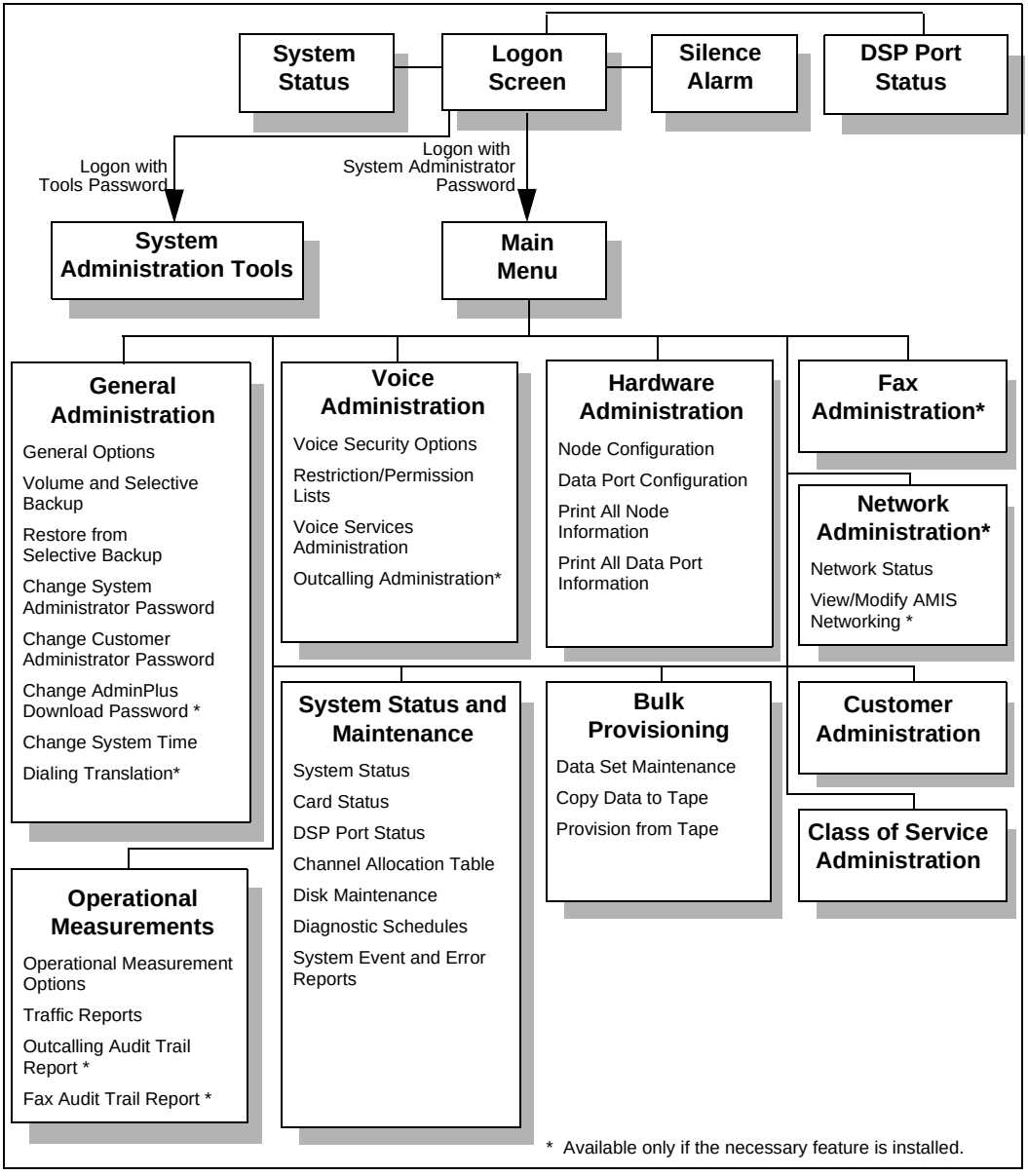
Risk of data loss

Do not remove the Multi-Customer feature from an operational system. Attempts to do so may result in loss of user information such as mailboxes and messages.

The system administration menu hierarchy

Menu hierarchy

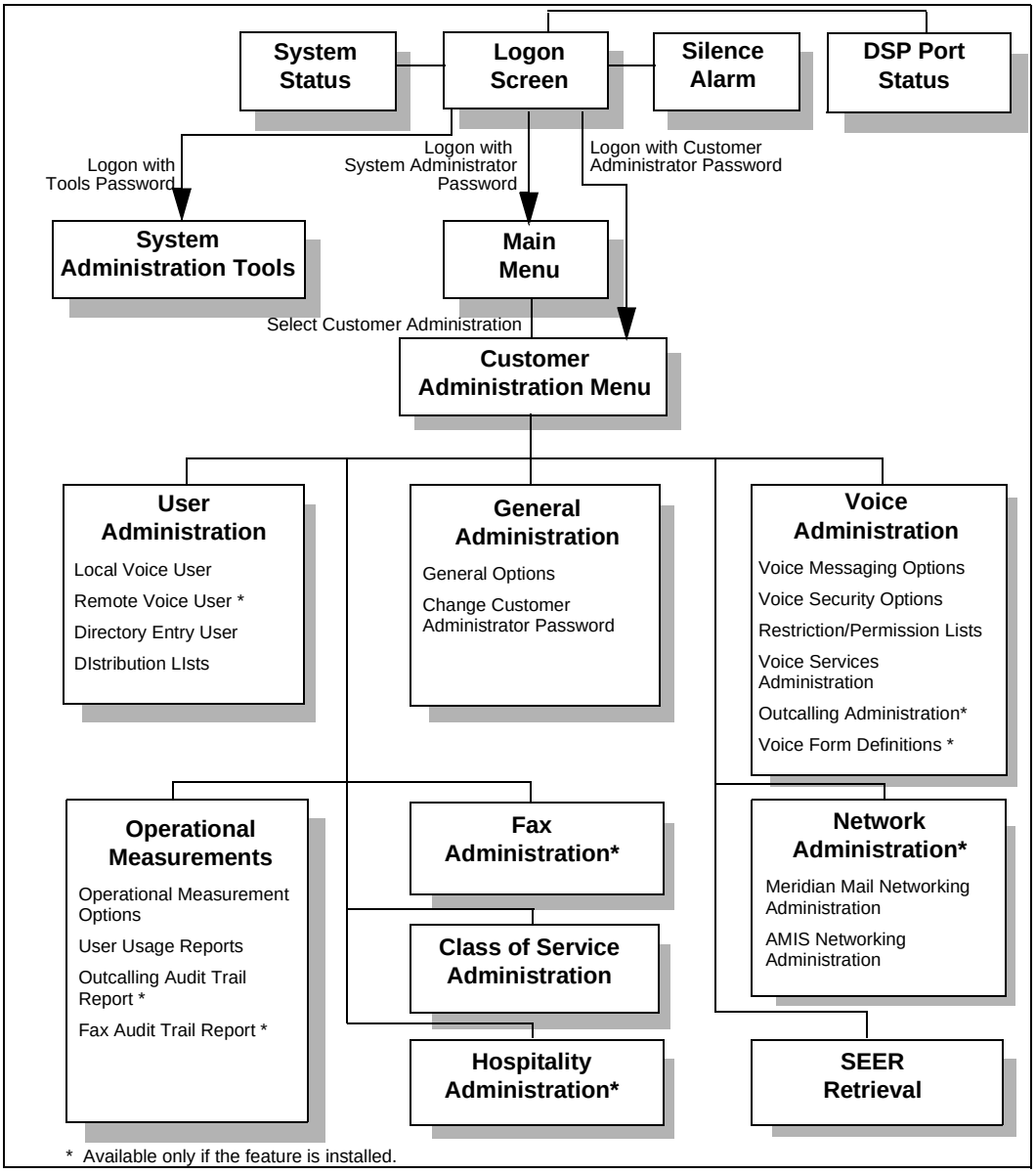
The following is an example of the system administration menu hierarchy.



The customer administration menu hierarchy

Menu hierarchy

The following diagram shows an example of the customer administration menu hierarchy. You can log on with either the system or customer administrator password.



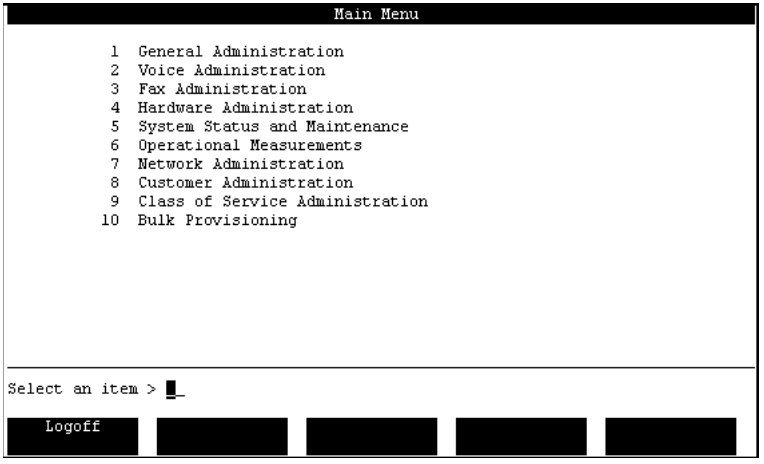
The Main menu

Introduction

The Main menu is the first screen that is displayed when you log on with the system administration password. This menu is your starting point for performing Meridian Mail system administration tasks.

The menu

Here is an example of the Main menu.



Feature-dependent items

The following menu items are displayed only if the appropriate feature is installed:

- Fax Administration is displayed if Fax on Demand is installed.
- Network Administration is displayed if Meridian Networking or AMIS Networking, or both, are installed.

The Customer Administration menu

Introduction

The Customer Administration menu is displayed when you

- log on with the customer administrator password and select a customer

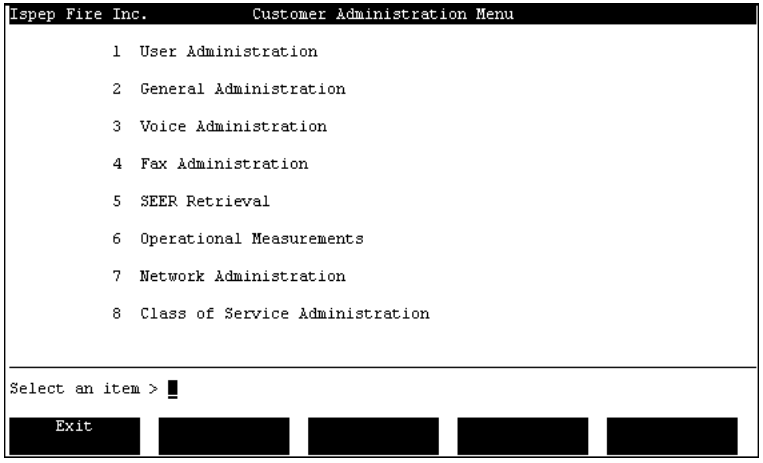
  or

- log on with the system administrator password, choose Customer Administration from the Main menu, and select a customer

The Customer Administration menu is your starting point for performing Meridian Mail customer administration tasks.

The menu

This is an example of the Customer Administration menu.



Feature-dependent items

The following menu items are displayed only if the appropriate feature is installed:

- Fax Administration is displayed if Fax on Demand is installed.
- Network Administration is displayed if Meridian Networking or AMIS Networking, or both, are installed.
- Hospitality Administration is displayed if Hospitality Voice Messaging is installed.

User administration

Description

User administration involves creating and maintaining a database of users.

Administration level

All users must be added to customers. Distribution lists are also customer specific. Therefore, all User Administration tasks are performed at the Customer Administration level only.

Local voice users

Local voice users have mailboxes. You can add, modify, and delete local voice users in User Administration. You can also carry out other user-related functions such as recording personal verifications and setting up remote notification schedules.

Remote voice users

If Meridian Networking or Enterprise Networking, or both, are installed, you can add users at remote sites to your local user database. One way of adding and deleting remote voice users is through User Administration.

Remote voice users can be added to distribution lists at the local site. Local users can use name dialing and call sender to call remote voice users and name addressing to compose messages to them.

Directory entry users

Directory entry users do not have mailboxes. They are, however, in the user directory, and therefore can be accessed by features such as name dialing and Thru-Dial. These users are added, modified, and deleted from User Administration.

Distribution lists

Distribution lists contain a list of mailbox numbers. Whenever you send a message to a distribution list, it is sent to all of the mailboxes in the list.

Administering distribution lists involves

- assigning a number to each list
- adding mailbox numbers to each list
- keeping the lists up to date
- recording a personal verification for each list

General administration

Administration level

Some General Administration tasks are performed on the entire system, whereas others are specific to customers. You will, therefore, need to work from both the System Administration level and the Customer Administration level in order to complete General Administration.

Defining general options

The General Options screen is available from both System Administration and Customer Administration.

System administration

Some general options apply to the entire system. You can do the following at the System Administration level:

- Modify the system name, system number, and system addressing lengths.
- Choose the ACCESS default customer number.
- Choose the Integrated Mailbox Administration default customer number.
- View a list of installed features.
- Choose the date format for reports.
- Define the SEER printer and Reports printer port names.

Customer administration

Other general options are specific to each customer group. You can do the following at the Customer Administration level:

- Modify the customer name.
- Modify the customer type.
- Enable the following features (if installed) for each customer:
  - Voice Menus and Announcements
  - Voice Forms
  - Fax on Demand
  - Meridian Mail Networking
- Define the attendant DN.
- Assign up to 15 classes of service to each customer.

Backing up and restoring data

Administration level

You can back up and restore data from the System Administration level only.

Description

You can perform the following types of backups:

- full backups (of data and voice) to tape
- partial backups (of data only) to tape or disk (if the Disk to Disk Backup feature is installed)
- selective backups of users or services to tape

You can only restore users or services that were selectively backed up to tape from General Administration.

For information about restoring data from a full or partial backup, refer to the *System Installation and Modification Guide* (NTP 555-7001-215).

Changing passwords and the system time

System administration

You can change the following from the System Administration level:

- the system administrator password
- the customer administrator password
- the minimum password length for administration passwords
- the AdminPlus download password (if AdminPlus is installed)
- the system time

Customer administration

You can change only the customer administrator password at the Customer Administration level.

Setting up dialing translations

Administration level

If Fax on Demand or AMIS Networking, or both, are installed, you must set up translation tables. Translation tables apply to all customers and can only be configured at the System Administration level.

Description

These tables tell Meridian Mail how to translate collected digits (from an AMIS message header or a fax callback number entered by a caller) into a number that Meridian Mail can dial.

Voice administration

Administration level

Some Voice Administration tasks are performed on the entire system, whereas others are specific to customers. You will, therefore, need to work from both the System Administration level and the Customer Administration level in order to complete Voice Administration.

Defining voice messaging options

Administration level

All voice messaging options are customer specific and are modified at the Customer Administration level only.

Description

Defining voice messaging options involves the following tasks:

- If more than one language is installed, you must define the default language and whether it overrides users' preferred languages.
- If Dual Language Prompting is installed, you must define the secondary language in which prompts are played.
- You can record customized versions of the call answering greeting (MMUI) and VMUIF tutorials.
- You can enable or disable name dialing/name addressing and external call sender.
- You can define operational characteristics for voice messaging such as
  - the maximum delay for timed delivery
  - the broadcast mailbox number
  - the maximum number of days that read messages are retained
  - the playback speeds that mailbox users can apply to individual mailbox messages

Defining voice security options

Defining voice security options is extremely important in order to safeguard your system from unauthorized use and abuse by hackers and users.

The Voice Security Options screen is available at both the System Administration level and Customer Administration level. However, different parameters are modified at each level.

System administration

You can do the following at the System Administration level:

- Suppress telset display of passwords as they are entered.
- Set up monitoring periods for
  - system accesses
  - thru-dials
  - specific internal or external calling line IDs (CLIDs), or both

Customer administration

You can do the following at the Customer Administration level:

- Select the restriction/permission list for Call Answering/ Express Messaging Thru-Dial.
- Make mailbox passwords more secure by
  - defining a password prefix
  - specifying the minimum password length
  - forcing users to change their passwords the first time they log on
- Specify the maximum number of invalid logon attempts that are allowed before a mailbox is disabled or a call session is terminated.

Defining restriction/ permission lists

Administration level

Restriction/permission lists are created at the System Administration level only. The same lists are available to all customers.

Description

Restriction/permission lists are another very important part of ensuring system security. A restriction/permission list specifies which dialing codes are not allowed, thereby preventing users or callers from placing calls to unauthorized numbers such as domestic long distance numbers or international numbers.

You can define up to 80 different restriction/permission lists that can then be applied to different features that place outcalls such as call sender, Thru-Dial, Remote Notification, and AMIS networking.

Performing voice services administration

The Voice Services Administration menu is available at both the System Administration level and Customer Administration level.

The VSDN Table

This is where you add voice service DNs (VSDNs) for each service that you want to make directly dialable by a unique number. VSDNs are specific to each customer.

At the Customer Administration level, you can add, modify, and delete VSDNs.

At the System Administration level, you can modify and delete existing VSDNs. You cannot add new VSDNs.

The Voice Services Profile

The Voice Services Profile is accessible at the Customer Administration level only. This is where you define characteristics for voice services such as

- timeouts
- holidays (used by time-of-day controllers)

Voice service and fax item definitions

You can add, modify, and delete the following voice and fax services at the Customer Administration level:

- announcement definitions
- thru-dial definitions
- time-of-day controller definitions
- voice menu definitions
- fax item definitions

You can modify and delete existing definitions (but not add new ones) from the System Administration level. These voice and fax services are specific to each customer.

Setting display options

You can set display options at the System Administration level only.

Display options allow you to choose

- how you want information sorted in Voice Services Administration screens
- whether the Choice of Services and Menu Actions lists are displayed

Performing outcalling administration

Outcalling includes the Remote Notification (RN) and the Delivery to Non-User (DNU) features. If installed, you must check that the default settings are acceptable, or change them to suit your needs.

System administration

Only one field, Maximum Number of Outcalling Channels, is configured at the System Administration level.

Customer administration

All other Outcalling Administration is customer specific.

Remote Notification parameters include

- the maximum number of remote notification retry repeats
- the numeric pager data terminator

Delivery to Non-User parameters include

- allowed delivery times for weekdays and weekends
- retry limits and intervals for busy, unanswered, and answered conditions
- the number of times to play a DNU message

Defining voice forms

Administration level

Voice forms are specific to customers. Voice form definitions, therefore, are created and maintained at the Customer Administration level only.

Description

Creating voice forms involves setting operational characteristics for each voice form as a whole, recording all of the prompts (known as fields), and setting field-specific operational characteristics.

Hardware administration

Introduction

Almost all of the screens in Hardware Administration are read-only. They are for viewing purposes only.

To modify your hardware configuration, you must log on to the Tools level and access the Modify Hardware tool. For more information, refer to *Meridian Mail System Administration Tools* (NTP 555-7001-305).

Administration level

Hardware Administration is available at the System Administration level only.

Node configuration

You can view the number of nodes that are installed and the types of cards that have been configured for each node.

Data port configuration

You can view configurations for the following data ports:

- MMLink
- Terminal
- Printer
- PMS
- Modem
- MSLink (for Meridian Mail AutoAdmin)
- AdminPlus (if installed)
- NWModem

Note: You can modify the Network Modem DN from Hardware Administration.

Printing information

You can print all node and all data port information.

System status and maintenance

Introduction

System Status and Maintenance primarily involves viewing the status of the system and various hardware components to see if everything is operational.

When a hardware component needs servicing, it must first be disabled and then reenabled when the problem is fixed. This is done in System Status and Maintenance.

Administration level

System Status and Maintenance is available at the System Administration level only.

Viewing status and disabling components

For each of the following hardware components, you can view its status, disable (or courtesy disable) it for servicing, and reenable it:

- the entire system
- nodes
- cards
- DSP ports

Channel Allocation Table

The Channel Allocation Table shows how channels (ports) are allocated to services.

From the Channel Allocation Table, you can view the following:

- the channels that are on your system, their type, and whether they are shared by services or dedicated to a particular service for placing outbound calls
- the maximum number of each type of port, and how many of each port type have been allocated

Channel Allocation Table (cont'd)

If you disable ports, you can do the following:

- Modify the Primary DN.
- Modify Channel DN.
- Modify the port type and capability.
- Dedicate ports to a particular customer (for outcalls only).
- Dedicate ports to a particular service (for outcalls only).

Disk maintenance

Shadowed systems

On shadowed systems, you can do the following from the Disk Maintenance screen:

- View the status of the prime and shadow disks in a disk pair.
- Disable and enable a disk.
- Perform diagnostics.

Unshadowed systems

On unshadowed systems, you can view the status of the prime disk and perform diagnostics.

Diagnostic schedules

You can schedule diagnostics to occur at a specific time on certain days. You can specify the following about the scheduled diagnostics:

- whether voice path diagnostics should be performed, and other related parameters

System event and error reports

You can perform the following tasks from the System Event and Error Reports menu.

SEER retrieval

If you do not want all SEERs to be retrieved, you can specify which SEERs should be retrieved according to SEER class, severity level, or SEER type.

Note: SEER retrieval is available at the System Administration and Customer Administration levels.

SEER configuration

From the SEER Configuration screen, you can do the following:

- Specify the mailbox (the message trigger mailbox) to which you want messages to be sent when a SEER that meets a specific criteria is generated. This allows you to be notified immediately of SEERs that you consider to be critical.
- Set SEER throttling parameters which allow you to prevent SEERs that are duplicated a certain number of times from being sent to the printer or message trigger mailbox, or both.
- Set SEER escalation parameters which allow you to specify how many times a SEER needs to be duplicated before it is escalated to the next severity level.
- Set the SEER filtering levels which allow you to control which SEERs are sent to the printer and message trigger mailbox (according to type and severity level).

SEER remapping

SEER remapping allows you to remap the severity level of up to 60 SEERs to a different severity level and have that information stored on disk.

For example, a SEER that is classified as major in Meridian Mail may be critical to your particular system. You could, therefore, remap this SEER as critical.

Operational measurements

Introduction

There are three kinds of operational measurement reports: traffic reports, user usage reports, and audit trail reports.

Administration level

Some of these reports are accessible from the System Administration level, whereas others are accessible from the Customer Administration level.

Operational measurement options

Administration level

Operational measurement options are modified at the System Administration level only. The Operational Measurement Options screen is available at the Customer Administration level, but it is read-only.

Description

Setting operational measurement options involves specifying

- whether to collect traffic, user usage, session trace, and audit trail data
- the start and end times for the traffic period
- the number of days traffic data, user usage data, and audit trail data are stored

Traffic reports

Administration level

Traffic reports report on the entire system, not specific customers, and, therefore, are accessible from the System Administration level only.

Description

You can view or print a summary of traffic report services that shows the number of accesses, the average length, and voice mail usage.

Traffic reports (cont'd)

You can view or print more detailed traffic reports for the following:

- Voice Messaging
- Channel Usage
- Services
- Networking
- AMIS Networking
- Outcalling
- Fax
- Disk Usage

You can view or print statistics for the following:

- Hospitality
- Guest Console

User usage reports

Administration level

Since users belong to specific customers, user usage reports are accessible at the Customer Administration level only.

Description

You can view or print user usage reports which provide local usage data, Meridian network usage data, and AMIS network usage data.

Audit trail reports

Administration level

Outcalling and Fax audit trail reports can be generated from both administration levels. When generated at the System Administration level, the data is for the entire system. When generated at the Customer Administration level, the data is specific to the selected customer.

Outcalling audit trails

If Outcalling is installed, you can view or print summary reports that show the target DNs to which users are sending DNU messages and remote notifications as well as the status of each call.

You can also view or print more detailed reports that also show the channel DN that was used and how many retries there were.

Fax audit trails

If Fax on Demand is installed, you can view or print summary reports that show the called DN, billing DN, duration, and status of each fax call.

You can also view or print more detailed reports that show the channel DN that was used and how many retries there were.

Class of Service administration

Introduction

Before you can add local voice users, you must create your classes of service (COS). Each local voice user must be assigned to an already defined class of service.

Administration level

Classes of service can be added, modified, and deleted at the System Administration level only.

At the Customer Administration level, classes of service can be viewed only.

COS-controlled features

Classes of service determine the feature capabilities of the local voice users assigned to them. Some examples of features and limits that are controlled by classes of service are

- the voice storage limit
- the maximum length of composed messages
- the maximum length of call answering messages
- the ability to send broadcast and network broadcast messages
- notification of busy line to callers
- delivery to non-user (DNU) capability and related DNU parameters
- remote notification (RN) capability and related RN parameters
- the ability to receive and send AMIS open network messages
- the restriction/permission lists that are applied to AMIS open networking, extension dialing, and custom revert

Maintaining classes of service

Maintaining classes of service involves modifying classes of service as needed. Whenever a change is made to a class of service, the change is propagated to all users belonging to that class of service.

It also involves deleting classes of service that are no longer needed (and reassigning users to another class of service before you delete).

Fax administration

Administration of the Fax on Demand service

Fax Administration is available only if Fax on Demand is installed. It involves configuring parameters for the Fax on Demand service.

Fax Administration is available at the System Administration and Customer Administration levels. However, most of the setup is done at the Customer Administration level.

System administration

Only one parameter is configured at the System Administration level:

- the maximum number of fax delivery channels

Customer administration

The remainder of the Fax Administration parameters are customer specific and, therefore, are configured at the Customer Administration level:

- the maximum resolution of fax reception (normal or fine)
- the maximum number of pages allowed per fax item
- fax delivery retry limits and intervals for cases where fax items cannot be delivered (due to transmission errors or no carrier availability)
- allowed times for delivery of fax items on weekdays and weekends
- the delivery time limit

Creating fax items

Fax items are not created in Fax Administration. You must access the Voice Services Administration menu at the Customer Administration level to add fax item definitions.

Network administration

Description

Network administration involves the administration of Meridian Networking, Enterprise Networking, and AMIS Networking.

Meridian Networking and Enterprise Networking

Administration level

If Meridian Networking or Enterprise Networking, or both, are installed, all administration is done at the Customer Administration level since Meridian Networking and Enterprise Networking can be enabled for only one customer.

Description

Administration of the Meridian Networking and Enterprise Networking features involves

- local site maintenance
- remote site maintenance, which involves adding remote sites, specifying the networking protocol and dialing plan for each site, and recording a spoken site name
- network configuration, which involves setting initiation times, holding times, stale times, the batch threshold, and wakeup interval
- performing a modem verification test
- checking the network status periodically

AMIS and Virtual Node AMIS Networking

Administration of the AMIS Networking feature takes place at both the System Administration and Customer Administration levels.

System administration

At the System Administration level, you can access the View/ Modify AMIS Networking Information screen to

- enable or disable incoming and outgoing messages
- specify the allowed delivery times for outgoing messages
- specify the initiation time, holding times, stale times, batch threshold, and wakeup interval

You can also check the status of the AMIS Networking service.

Customer administration

At the Customer Administration level, you can access the AMIS Networking Administration screen to define

- the AMIS compose prefix
- the number of messages to transmit per session
- the system access number

Hospitality administration

Introduction

Hospitality Administration is available only if the Hospitality Voice Messaging feature is installed.

Administration level

Since Hospitality Voice Messaging can be enabled for one customer only, Hospitality Administration is accessible from the Customer Administration level only.

Hospitality profile

The Hospitality Profile screen is where you define parameters for all Guest Messaging services. Some examples are

- the initial guest password length
- whether the initial guest password is generated using the guest's last name or the check-in date
- Post Check-out Mailbox settings
- customizable greetings for
  - the guest logon greeting
  - unanswered and busy guest phones
  - vacant rooms
  - rooms that do not have voice messaging

Modifying mailboxes

You can view or modify a guest mailbox from Hospitality Administration. You can modify settings such as

- room number and status
- the guest's first and last name
- autologon
- the revert DN

Changing the GAC password

You should change the default GAC password after installation and continue to change it on a regular basis.

Hospitality system status

You can view the status of the Hospitality system, including the links from Meridian Mail to the PMS (if there is one) and the Meridian 1.

Hospitality install parameters

Modifying install parameters involves

- setting PMSI parameters
- setting SL-1 link parameters
- setting voice count parameters
- configuring the language identifier table
- providing international character mapping for the PMSI link

Section B: Understanding menus, screens, and keys

In this section

Overview	2-36
Keypad functions	2-38
Meridian Mail menus	2-39
Meridian Mail screens	2-42
Getting around in screens	2-44
Entering information in fields	2-45
Softkeys	2-51
Getting help	2-52
Error messages	2-53

Overview

Introduction

System administration menus and screens have a consistent format. The way in which items are selected and data is entered is the same for all menus and screens.

In this section

This section describes

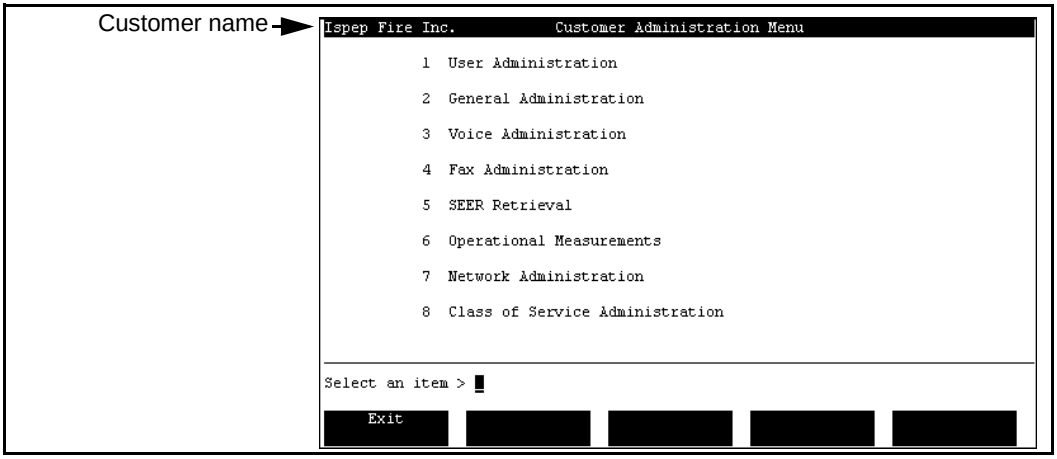
- keypad functions
- the layout of menus
- the layout of screens
- types of fields
- how to select menu items
- how to select options and enter data in fields
- how to navigate through fields in screens
- how to scroll through multipage screens
- softkeys
- how to get help

Customer Administration menus and screens

All menus and screens that are displayed at the Customer Administration level display the name of the selected customer in the upper left-hand corner of the screen.

Example

This is a menu at the Customer Administration level.



Keypad functions

Application mode

When the keypad is in application mode, certain functions are available on the keypad when you press single keys or key combinations. Application mode is the default whenever the system is rebooted.

Supported terminals

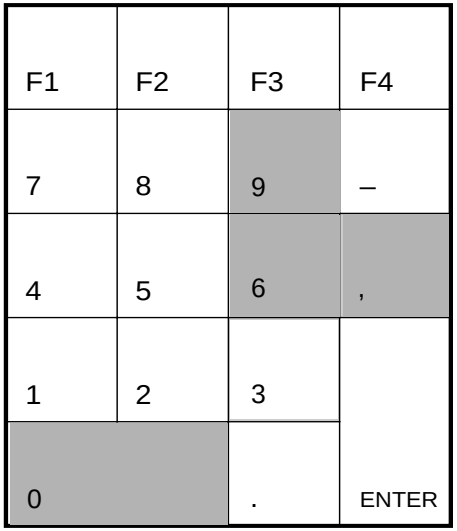
Keypad functions are supported on VT220 terminals and the following VT200-compatible terminals: VT320, VT420, HP700/22, and HP700/32.

Numeric keypad

If you choose to work with a numeric keypad (where the numeric keys generate numbers when you press them), then only the F1, F2, F3, and F4 keys retain the functions indicated. The keypad is set to numeric mode through the terminal's setup function.

Keypad function key positions

The following illustration shows the functions available when the keypad is in application mode.



F1 - Softkey 1
F2 - Softkey 2
F3 - Softkey 3
F4 - Softkey 4
1 - Start of field
2 - Next word in field
3 - End of field
4 - Previous field
5 - Next field
7 - Previous page
8 - Next page
\- - Delete field contents
. - HELP
ENTER - Softkey 5

(shading indicates that the key does not have a function)

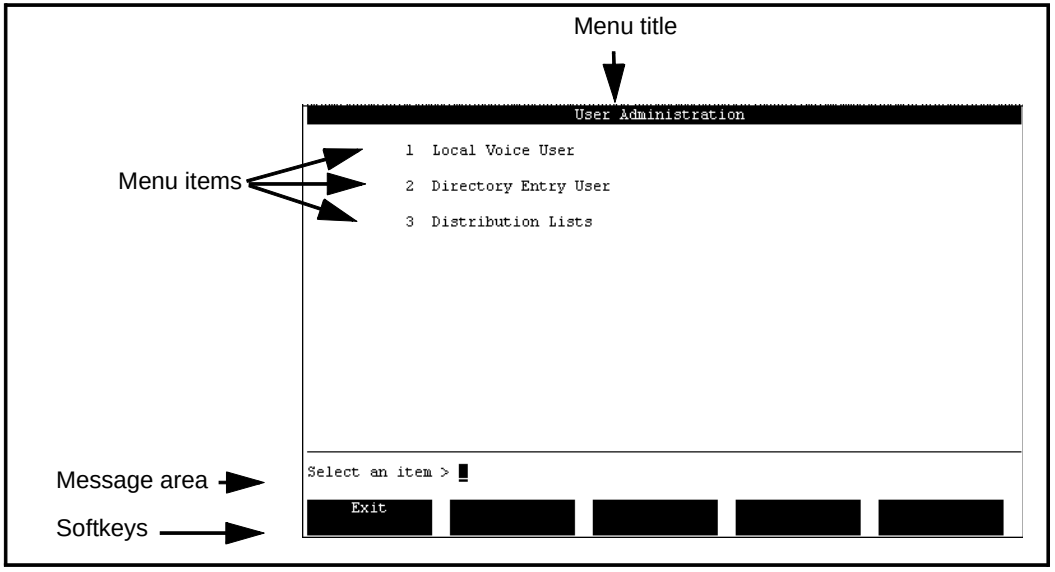
Meridian Mail menus

Description

A menu presents a list of items from which you can choose. When an item is selected, either another menu or a screen is displayed.

A typical menu

The following is an example of a menu.



Parts of a menu

This table describes the parts of a menu.

Part	Description
Menu title	Menu titles are always on the first line.
Menu items	Each menu has a list of choices that are preceded by numbers. These are menu items from which you can choose. Choosing a menu item causes either another menu or a screen to be displayed.
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.

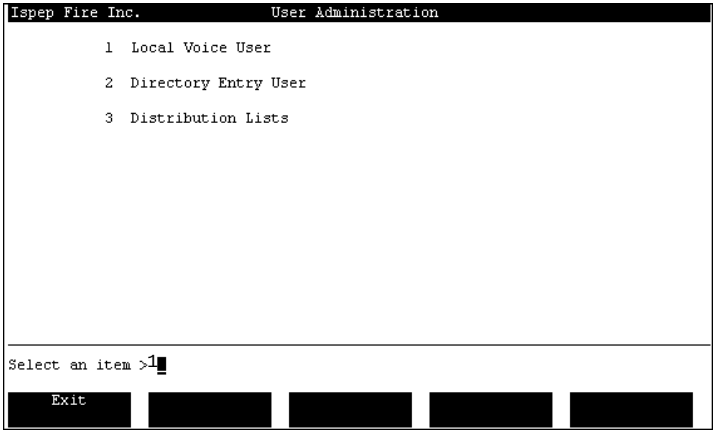
Choosing a menu item

Each item in a menu has a number. The system displays a prompt requesting you to make a selection from the items presented.

To select a menu item, follow these steps.

Starting Point: Any menu with the “Select an item” prompt displayed

Step	Action
1	Enter the number that corresponds to the item you want to choose and press <Return>. **Example:** You want to add local voice users to your system so you enter 1 and press <Return>.



Result: Another menu or a screen is displayed.

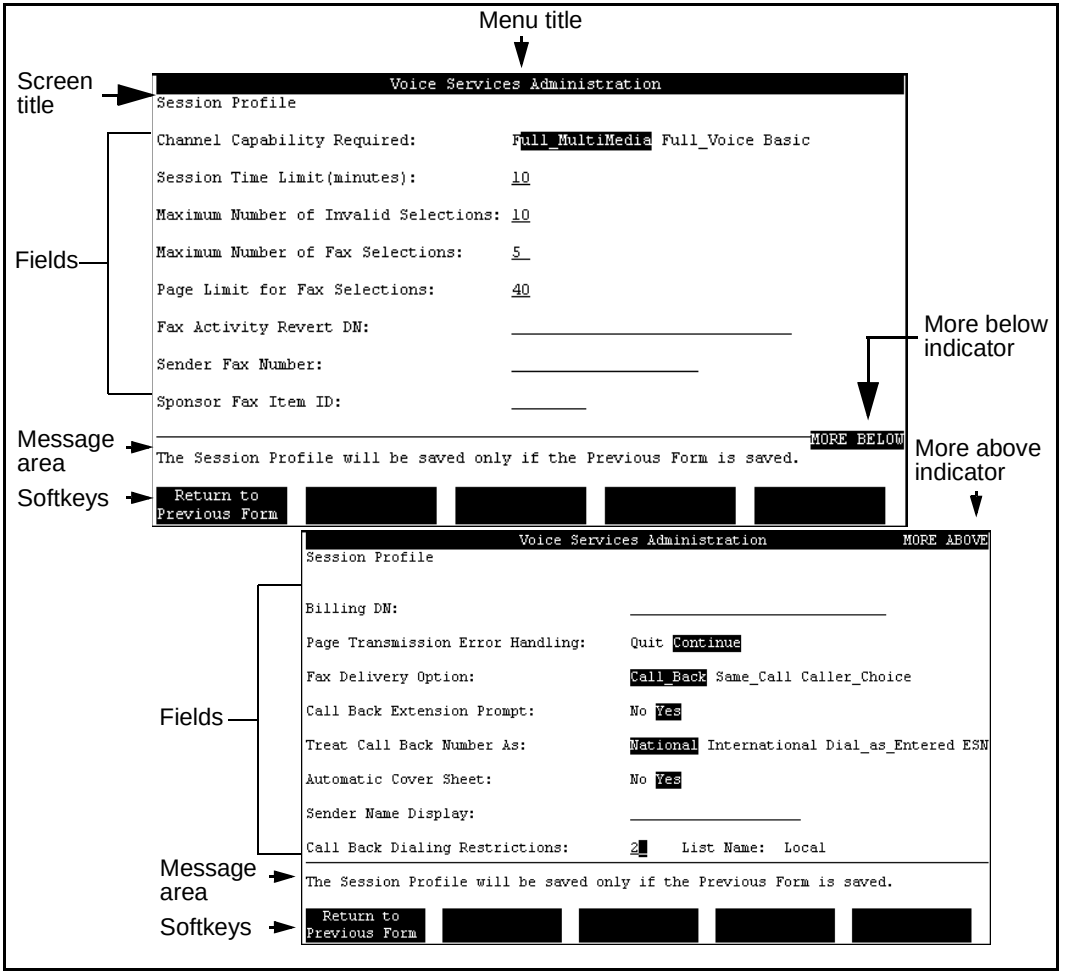
Meridian Mail screens

Description

Screens contain fields in which you can either make selections or enter data. It is by filling in fields that you customize Meridian Mail to meet your requirements and suit your needs.

A typical screen

The following is an example of a screen.


Menu title
Screen title
Voice Services Administration
Session Profile
Channel Capability Required: Full_MultiMedia Full_Voice Basic
Session Time Limit(minutes): 10
Maximum Number of Invalid Selections: 10
Maximum Number of Fax Selections: 5
Page Limit for Fax Selections: 40
Fax Activity Revert DN:
Sender Fax Number:
Sponsor Fax Item ID:
Fields
More below indicator
MORE BELOW
Message area
The Session Profile will be saved only if the Previous Form is saved.
Softkeys
Return to Previous Form
More above indicator
Voice Services Administration
MORE ABOVE
Session Profile
Billing DN:
Page Transmission Error Handling: Quit Continue
Fax Delivery Option: Call_Back Same_Call Caller_Choice
Call Back Extension Prompt: No Yes
Treat Call Back Number As: National International Dial_as_Entered ESN
Automatic Cover Sheet: No Yes
Sender Name Display:
Call Back Dialing Restrictions: 2 List Name: Local
Fields
Message area
The Session Profile will be saved only if the Previous Form is saved.
Softkeys
Return to Previous Form

Parts of a screen

This table describes the parts of a screen.

Part	Description
Menu title	This is the name of the menu from which the screen was accessed.
Screen title	The name of the screen.
Fields	Fields in screens are much like fields in forms. You can either enter information in them, or select from a predetermined set of options. It is by filling in fields that you define how you want Meridian Mail to work and customize the system to meet your needs.
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.
More below indicator	This indicator is displayed in multipage screens. It indicates that there are more fields below the last field that is currently displayed.
More above indicator	This indicator is displayed in multipage screens. It indicates that there are more fields above the first field that is currently displayed.

Getting around in screens

Navigating between fields

The following keys on the keyboard and on the application keypad (see “Keypad functions” on page 2-38) move the cursor between fields.

IF you want to	THEN press
move to the next field	• the Tab key • the down arrow key • the Return key, or • 5 on the application keypad.
move to the previous field	• the up arrow key, or • 4 on the application keypad.

Moving through multipage screens

Certain screens contain more fields than can be displayed at one time on the display terminal. You can view additional pages in one of two ways: by scrolling and by paging.

Scrolling

If you see “More Below” at the bottom of a screen or “More Above” at the top of a screen, you can use the following keys.

IF you want to	THEN press the
view the next page of a multipage screen	• Next Scrn hardkey.
view the previous page of a multipage screen	• Prev Scrn hardkey.

When the “More Below” prompt disappears, you are at the end of the screen. When the “More Above” prompt disappears, you are at the top of the screen.

Using the down arrow key

The down arrow key displays only the last input field, even if there is instructional text below it. To view any text that may appear at the end of a screen, use the Next Scrn hardkey.

Paging

In some screens, a [Next Page] softkey is displayed that can be used to move between the pages of a screen.

Entering information in fields

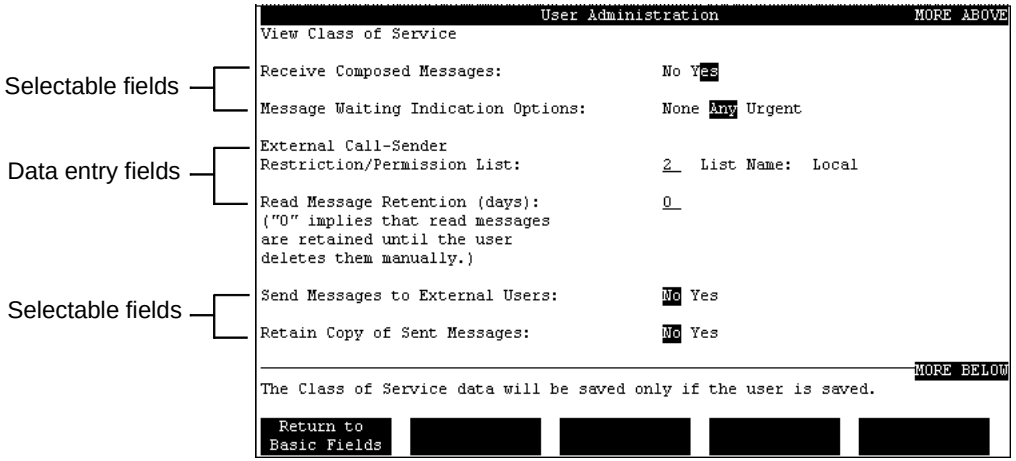
Introduction

Information is entered in the fields of Meridian Mail screens. There are two types of fields:

- selectable fields
- data entry fields

Example

This screen contains both types of fields.


Selectable fields
Data entry fields
Selectable fields
User Administration
MORE ABOVE
View Class of Service
Receive Composed Messages: No Yes
Message Waiting Indication Options: None Any Urgent
External Call-Sender
Restriction/Permission List: 2 List Name: Local
Read Message Retention (days): 0
("0" implies that read messages
are retained until the user
deletes them manually.)
Send Messages to External Users: No Yes
Retain Copy of Sent Messages: No Yes
MORE BELOW
The Class of Service data will be saved only if the user is saved.
Return to
Basic Fields

Selectable fields

Selectable fields present a number of predefined options from which you can choose.

The option that is in reverse video (light text on a dark background) is the selected option.

After installation, selectable fields always have one of the options selected as the default.

Examples

Examples of selectable fields in the above screen example are Receive Composed Messages and Retain Copy of Sent Messages.

Choosing an option in a selectable field

To choose a predefined option in a selectable field, follow these steps.

Step	Action
1	Move the cursor to the field you want to modify.
2	Use the right (and left) arrow keys, or the spacebar, to select the option you desire. **Note:** The selected option appears in reverse video.

Data entry fields

You type information, such as titles and numbers, into data entry forms. There are often limitations placed on data entry fields, such as the types of characters you can enter or a range of numbers. Data entry fields are indicated by an underline next to the field name. This is where you enter information.

Some of these fields are prefilled with default values. These values can be changed as needed. Others are blank by default and require an entry.

Example

An example of a data entry field (on page 2-45) is the Read Message Retention (days) field.

Entering information in a data entry field

To enter information in a data entry field, follow these steps.

Step	Action
1	Move the cursor to the field you want to modify.
2	Is there currently any information in the field? • If yes, go to step 3. • If no, type the information in the field.
3	Delete the current content of the field.
4	Type the information in the field.

IF you want to	THEN press
clear the current contents	the <Remove> key.
delete one character to the left of the cursor	the <x> key.
delete the character on which the cursor is positioned	the <Back Space> key.

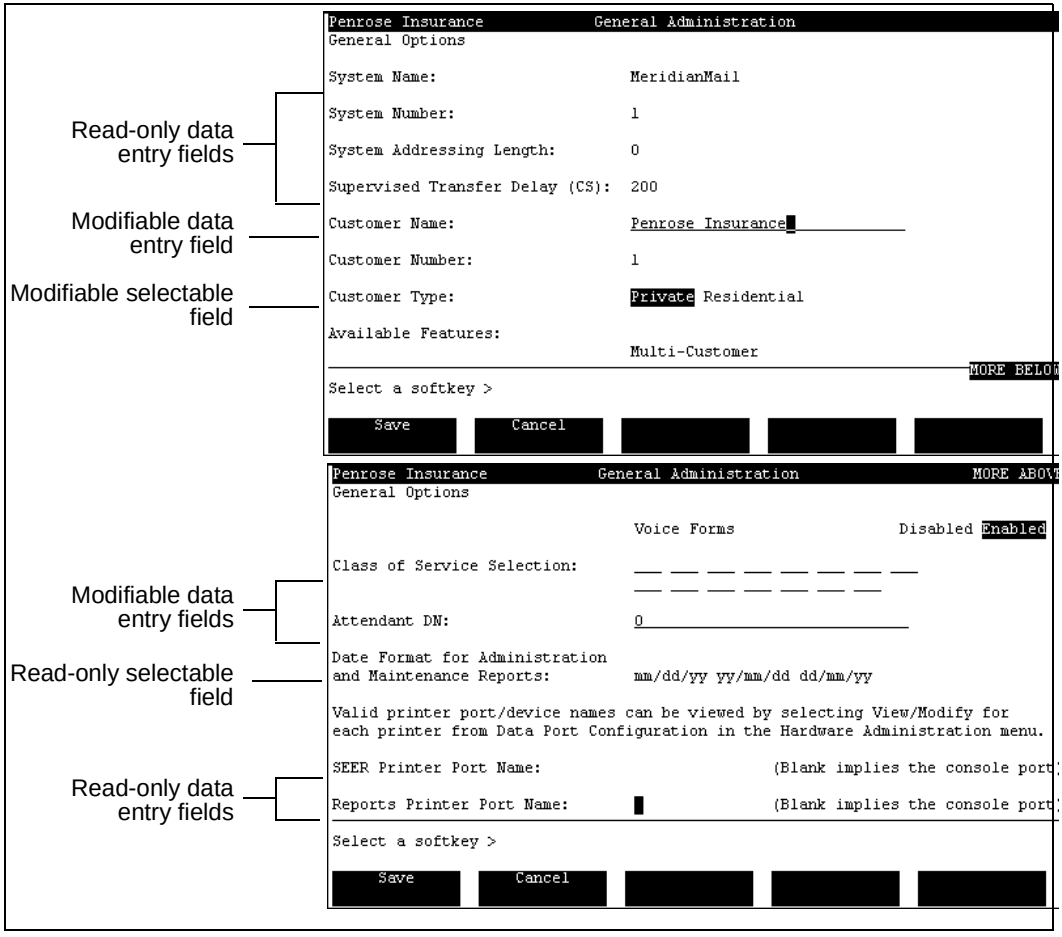
Modifiable versus read-only fields

Some fields are read-only and cannot be modified. This table describes the conventions that are used to indicate whether a field can be modified or is read-only.

Field type	Modifiable indicators	Read-only indicators
Selectable	Selected option is in reverse video	Selected option is in bold
Data Entry	Underlining	No underlining

Example

This screen has modifiable and read-only data entry fields, as well as a modifiable and read-only selectable field.


Read-only data entry fields
Modifiable data entry field
Modifiable selectable field
Modifiable data entry fields
Read-only selectable field
Read-only data entry fields
Penrose Insurance General Administration
General Options
System Name: MeridianMail
System Number: 1
System Addressing Length: 0
Supervised Transfer Delay (CS): 200
Customer Name: Penrose Insurance
Customer Number: 1
Customer Type: Private Residential
Available Features:
Multi-Customer
MORE BELOW
Select a softkey >
Save
Cancel
Penrose Insurance General Administration MORE ABOVE
General Options
Voice Forms Disabled Enabled
Class of Service Selection:
Attendant DN: 0
Date Format for Administration and Maintenance Reports: mm/dd/yy yy/mm/dd dd/mm/yy
Valid printer port/device names can be viewed by selecting View/Modify for each printer from Data Port Configuration in the Hardware Administration menu.
SEER Printer Port Name: (Blank implies the console port)
Reports Printer Port Name: (Blank implies the console port)
Select a softkey >
Save
Cancel

Selecting an entire line

In some screens, especially those that provide a list of things from which to choose, you need to select an entire line to indicate on which item you want to perform an action, and then press a softkey to indicate which action you want to perform.

To select an entire line in a screen, follow these steps.

Step	Action
1	Move the cursor to the line you want to select using the up and down arrow keys.
2	Press the spacebar. **Result:** The entire line is selected (as indicated by reverse video).

Prompt

Screens requiring this mode of selection often indicate this with the following prompt: “Move the cursor to the item and press the spacebar to select it.”

Example

You want to modify Customer 2. You, therefore, move the cursor to the line that reads Dennet & Sons and press the spacebar. The entire line is selected, as indicated by reverse video. You then press the View/Modify softkey to access the Customer Administration menu for that customer.

Mandatory fields

Certain data fields require you to insert values, whereas other fields are optional. Mandatory fields are identified in the field descriptions.

If you do not fill in a mandatory field and then try to save your settings, the system does not save the screen but, instead, prompts you to fill in the necessary field.

Softkeys

Description

Softkeys appear on the bottom two lines of menus and screens and are displayed in reverse video (light characters on a dark background).

They correspond to function keys F1 through F5 or F6 through F10 on the top row of the keyboard. The softkeys change according to the menu or screen. They may also change with the function you are performing.

Purpose

Softkeys are always actions. When you select a softkey, you are performing a function.

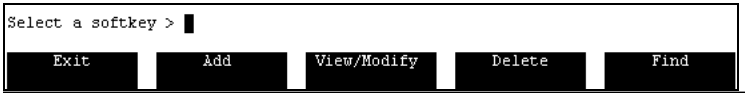
Common softkeys

The following softkeys occur frequently on the administration screens:

- [Exit]
- [Add]
- [View/Modify]
- [Delete]
- [Find]
- [Save]
- [Cancel]

Softkey positions

If any of these keys occur on a screen, they typically occur in the following positions.



Getting help

Introduction

Online help is available for most of the menus and screens, including the Main Menu.

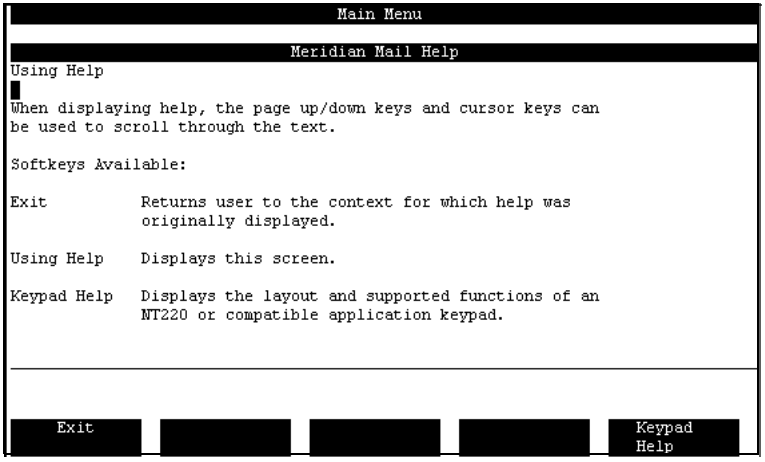
Procedure

To get Help, follow these steps.

Step	Action
1	Press the Help key. **Result:** The system displays explanations of the fields on the menu or screen in which you are working.
2	Once you are done reading the Help information, press the [Exit] softkey to return to the menu or screen.

A typical Help screen

The following shows an example of a Help screen.


Main Menu
Meridian Mail Help
Using Help
When displaying help, the page up/down keys and cursor keys can be used to scroll through the text.
Softkeys Available:
Exit Returns user to the context for which help was originally displayed.
Using Help Displays this screen.
Keypad Help Displays the layout and supported functions of an NT220 or compatible application keypad.
Exit
Keypad Help

Error messages

Introduction

The system displays error messages, both general and screen-specific, on the line above the softkey display.

These messages remain on the screen until the next user input or until another error message appears.

Purpose

These messages provide feedback on administration actions. They should not be confused with System Event and Error Report (SEER) messages.

SEER messages

If SEER printing is disabled, SEER messages will print out on the administration screen.

Examples of error messages

The following are two examples of error messages:

- "The key entered is not valid at this time."
- "Enter a number in the range of 1 to 6."

Section C: Meridian Mail features and interfaces

In this section

The main administration terminal and multiple administration terminals (MATs) 2-56

Meridian Mail feature availability 2-58

Meridian Mail telset interfaces 2-60

The main administration terminal and multiple administration terminals (MATs)

Introduction

Meridian Mail is administered through a menu-driven administration interface available at a terminal or personal computer (PC) using terminal emulation software. Using the administration menus, you establish the initial configuration of your system, maintain the user information base, create voice applications such as announcements and voice menus, monitor system usage and performance, and perform routine system maintenance.

The main administration terminal

All of these tasks are performed from the main administration terminal or from a PC using terminal emulation software.

Multiple administration terminals

The Multiple Administration Terminals (MATs) feature enables you to configure your main administration terminal and up to three secondary terminals, or MATs, on your system.

Tasks performed on MATs

Only a limited number of administrative tasks can be performed from a MAT. These include the following:

- User Administration

  You can perform all User Administration tasks, such as adding, modifying, and deleting users and distribution lists.
- Class of Service administration

  You can only view existing classes of service from a MAT. You cannot add, modify, or delete them.
- Voice Administration

  You can add, view, modify, and delete
  - voice service DNs
  - announcement and voice menu definitions
  - thru-dial definitions
  - time-of-day control definitions
  - fax item definitions

See also

For more information about configuring MATs, refer to the *System Administration Tools Guide* (NTP 555-7001-305).

Meridian Mail feature availability

Available platforms

This system administration guide is common to the following hardware platforms:

- Meridian Mail Modular Option
- Meridian Mail Modular Option EC

Both of these platforms are connected to a Meridian 1/SL-1 switch using an AML/CSL link.

Feature availability

Use the following table to determine whether you can install a particular feature on your system.

Feature	Meridian Mail Modular Option	Meridian Mail Modular Option EC
ACCESS	yes	yes
AdminPlus	yes	yes
AMIS Networking	yes	yes
Calling Line ID (CLID)	yes	yes
Disk Shadowing	yes	yes
Disk to Disk backup	yes	yes
Dual Language Prompting	yes	yes
Enterprise Networking	yes	yes
Fax on Demand	yes	yes
Hospitality	yes	yes
Integrated Mailbox Administration	yes	yes
Maximum number of languages supported	4	4
Meridian Mail AutoAdmin	yes	yes
Meridian Networking	yes	yes
Multiple Administration	yes	yes

Feature	Meridian Mail Modular Option	Meridian Mail Modular Option EC
Network Message Service (NMS)	yes	yes
Outcalling	yes	yes
Password Display Suppression	yes	yes
Single Terminal Access	yes	yes
Virtual Node AMIS Networking	yes	yes
VMUIF Voice Messaging	yes	yes
Voice Forms	yes	yes
Voice Menus	yes	yes
9600 bps Meridian Mail Interface	yes	yes

Meridian Mail telset interfaces

Introduction

Through the Meridian Mail telset interfaces, users interact with the Meridian Mail system to log in to their mailboxes, listen to messages, and compose and send messages.

Two telset interfaces

There are two Meridian Mail interfaces:

- Meridian Mail User Interface (MMUI)
- Voice Messaging User Interface Forum (VMUIF)

Customer and COS impacts

Both interfaces can be installed on a Meridian Mail system. However, only one interface can be enabled for each customer.

Each class of service must also specify which interface it supports. This means that you can assign only VMUIF classes of service to VMUIF customers, and MMUI classes of service to MMUI customers.

Definition: MMUI

The MMUI interface is a full-featured, command-driven Nortel proprietary voice mail interface. It is intended primarily for large business users.

Definition: VMUIF

VMUIF is a menu-driven interface. It is intended primarily for small business users, providing either full-featured voice messaging or only call answering and message retrieval.

VMUIF is also well suited to large campus environments such as universities or hospitals.

Terminology: users and subscribers

Users added to a customer for which the MMUI interface is enabled are referred to as *users.* Users added to a customer for which the VMUIF interface is enabled are referred to as *subscribers*, because they typically subscribe to a service through a central office.

Note: All of the Meridian Mail administration screens refer simply to users, even though user administration applies to both MMUI users and VMUIF subscribers.

Available features of MMUI and VMUIF

This table indicates which features are available for the two Meridian Mail user interfaces.

Feature	MMUI	VMUIF
handling of forwarded calls	yes	yes
personalized greetings	yes	yes
message waiting indication (MWI) support	yes	yes
remote notification (although user-changeable remote notification schedules from the telephone set are available only in the MMUI interface)	yes	yes
password-protected mailboxes	yes	yes
mailbox summaries and message playback	yes	yes
message reply, reply all, and message forward	yes	yes
personal distribution lists	yes	yes
message compose and send	yes	yes
AMIS Networking (if installed)	yes	yes
ability to assign a class of service (COS)	yes	yes
18-digit mailbox	yes	yes
mailbox Thru-Dial (A user can press **0** and dial a number while logged in to the mailbox.)	yes	
name addressing (A user can dial another user by name instead of by extension.)	yes	
Meridian Mail Networking (if installed)	yes	
Virtual Node AMIS Networking (if installed)	yes	
message tagging options (During message composition, a user can tag messages as urgent or for timed delivery.)	yes	
retention of sent or unsent messages	yes	
internal, external, and temporary greeting	yes	1 greeting
user-changeable personal verification	yes	yes
choice of identification (mailbox number or personal verification) to be played during call answering	yes	

Feature	MMUI	VMUIF
customizable customer greeting and customer attendant	yes	
custom operator revert	yes	
user-changeable remote notification schedules through the telephone set	yes	
express messaging	yes	
bilingual prompting (if more than one language is installed)	yes	
record, playback, and message tagging during call answering	yes	
speed control during message playback	yes	
adding to a recorded message	yes	
call answer only mailbox (Compose and Send must be disabled.)		yes
send only mailbox (Call Answering must be disabled.)		yes
rotary set interface (message retrieval with no DTMF input required)		yes
greeting change service (greeting change with no DTMF input required)		yes
introductory tutorial (special greeting on first access)		yes
volume control (DTMF control of default volume and volume setting)		yes
family mailboxes (Up to eight submailboxes can be administered through one telephone set.)		yes
“save as new” (Read messages can be reverted to “unread” or “new” status.)		yes
send on disconnect (implicit send command if a user hangs up after composing a message)		yes
mailbox resources (limiting receipt of messages based on mailbox resources)		yes
customizable login greeting		yes
disable reset (automated, timed reset of automated lockout resulting from password violation)		yes
editing capabilities for personal distribution lists	yes	
lockout revert (If locked out from the mailbox, a revert DN is possible.)		yes

Chapter 3

Logging on

In this chapter

Overview	3-2
Types of consoles	3-3
Logon/Status screen	3-4
Setting the system administration password	3-6
Setting the customer administration password	3-8
Changing the system administration password	3-10
Changing the customer administration password	3-12
Recovering a system administration password	3-14
Recovering a customer administration password	3-15
Logging on from the main administration terminal	3-17
Logging on from a MAT	3-19
Logging on from a remote terminal (non-EC system)	3-21
Logging on from a remote terminal (EC system)	3-24
Using a single terminal to access the M1 and Meridian Mail	3-29

Overview

Introduction

This chapter explains how to set your administration password and log on to the Meridian Mail system from the following types of consoles:

- the main administration terminal
- a multiple administration terminal (MAT)
- a remote terminal (non-EC system)
- a remote terminal (EC system)

After you are logged on, you can begin to work with the system administration menus, which are the starting point for general administrative functions and for customizing your system.

The chapter also describes how to change or recover your administration password.

Types of consoles

Introduction

Administrative functions can be carried out from the main administrative console for your Meridian Mail system or from a remote terminal connected to the system through a modem.

Multiple administration terminals

If the Multiple Administration Terminal feature is installed, your Meridian Mail system can support up to four administration terminals: one main administration terminal and up to three secondary terminals, or MATs.

Console types

The following table lists the types of consoles and their available features.

Main administration terminal	Multiple administration terminal	Remote terminal
installed with your system	available feature	available feature
all functions	user administration: add, modify, and delete mailboxes COS administration: view and find (read-only) voice services administration: add, view, modify, delete voice service DNs, announcement definitions, Thru-Dial definitions, time-of-day control definitions, and voice menu definitions	generally used by off-site service personnel to troubleshoot a system

Logon/Status screen

Description

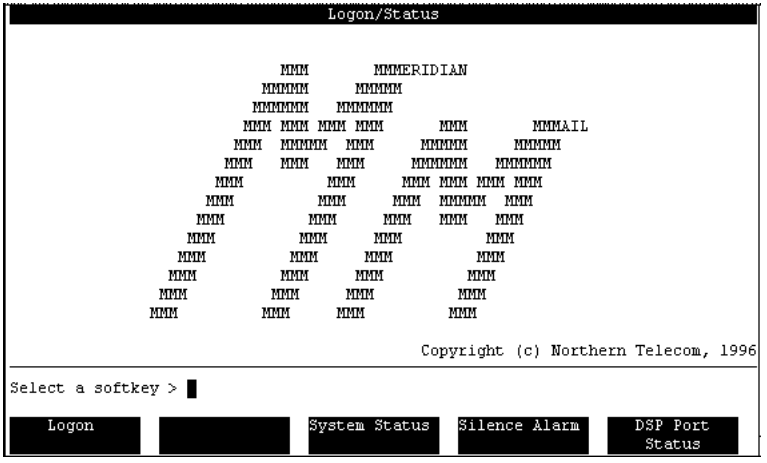
From this screen, you log on to the administration console to perform the following tasks:

- setting up and customizing your system
- carrying out administrative tasks either on a system-wide basis, or on a customer group or per-user basis
- configuring voice services
- viewing system status or DSP port status
- silencing alarms

The Logon/Status screen is displayed when the administration terminal is idle.

The Logon/Status screen

The following shows an example of the Logon/Status screen.



Note: When you log on at a MAT, only the [Logon] softkey is displayed.

ATTENTION

For security and memory usage reasons, do not leave the administration console unattended while you are logged on. Also, remember to log out at night. If you do not log out, critical audit and backup routines may not run because of insufficient memory.

Available softkeys

For information about the softkeys available from the Logon/ Status screen, see Chapter 29, "System status and maintenance".

Redrawing the Logon/ Status screen

If you power down your terminal and then power it back up, the screen may be drawn incorrectly. If the screen is corrupted, you see a row of "q"s (qqqqqqqqqqqqq) instead of the line near the bottom of the screen above the softkeys.

To redraw a corrupted screen, follow these steps.

Step	Action
1	Press <Ctrl> <w>. **Result:** A small window opens.
2	Type **if**. **Note:** You do not have to press <Return>. The "i" means initialize, and the "f" means full screen.

Setting the system administration password

Administration level

You can set the system administration password from the System Administration level only.

Overview

To log on to the Meridian Mail system from an administration terminal, you require a system administration password.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See "Setting the minimum password length for all administrator passwords" on page 17-7.)

Passwords are not case sensitive; even if you use capital letters when you define your password, you do not need to use capital letters when you type it.

Password security

For greater system security, your password should be no fewer than seven characters in length. A longer password is more difficult to guess than a shorter password.

For more information about ensuring the security of your system, see Chapter 7, "Setting up Meridian Mail security".

Procedure

To set your system administration password for the first time, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey. **Result:** The system prompts you for a password.
2	Type the default password **adminpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
3	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
4	Type your new password a second time, and press <Return>. **Result:** The system records the new password and displays the Main Menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 1 to step 4.

Setting the customer administration password

Administration level

You can set the customer administration password from the Customer Administration level.

Overview

To log on to the Meridian Mail system from a multiple administration terminal or a MAT, you require a customer administration password.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See "Setting the minimum password length for all administrator passwords" on page 17-7.)

Passwords are not case sensitive; even if you use capital letters when you define your password, you do not need to use capital letters when you type it.

Password security

For greater system security, your password should be no fewer than seven characters in length. A longer password is more difficult to guess than a shorter password.

For more information about ensuring the security of your system, see Chapter 7, "Setting up Meridian Mail security".

Note: Remember, there is only one customer password for the Customer Administration level. There is not one password per customer.

Procedure

To set your customer administration password for the first time, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey. **Result:** The system prompts you for a password.
2	Type the default password **custpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
3	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
4	Type your new password a second time, and press <Return>. **Result:** The system records the new password and displays the Main Menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 1 to step 4.

Changing the system administration password

Administration level

You can set the system administration password from the System Administration level only.

Introduction

To help ensure the security of your system, change the logon password regularly.

You can change the password only at the main administration terminal. The change is then automatically made to the configured MATs.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See "Setting the minimum password length for all administrator passwords" on page 17-7.)

For more information about ensuring the security of your system, see Chapter 7, "Setting up Meridian Mail security".

Procedure

To change your system administration password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration.
2	Select Change System Administrator Password. **Result:** The system prompts you to enter your existing administration password.
3	Type your existing password. **Note:** Your password is not displayed on the screen as you type it. **Result:** The system prompts you to enter a new password.
4	Type your new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
5	Type your new password a second time, and press <Return>. **Result:** The system records the new password, and you are returned to the General Administration menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat steps 2 to 5.

Changing the customer administration password

Administration level

You can change the customer administration password from either the System Administration level or the Customer Administration level.

Introduction

To help ensure the security of your system, change the logon password regularly.

You can change the password only at the main administration terminal. The change is then automatically made to the configured MATs.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See “Setting the minimum password length for all administrator passwords” on page 17-7.).

For more information about ensuring the security of your system, see Chapter 7, “Setting up Meridian Mail security”.

Note: Remember, there is only one customer password for the Customer Administration level. There is not one password per customer.

Procedure

To change your customer administrator password, follow these steps.

Starting Point: The Main Menu from the System Administration level or the Customer Administration Menu

Step	Action
1	Select General Administration.
2	Select Change Customer Administrator Password. **Result:** The system prompts you to enter your existing customer administration password.
3	Type your existing password. **Note:** Your password is not displayed on the screen as you type it. **Result:** The system prompts you to enter a new password.
4	Type your new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
5	Type your new password a second time, and press <Return>. **Result:** The system records the new password, and you are returned to the General Administration menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat steps 2 to 5.

Recovering a system administration password

Introduction

This topic describes how to restore a password that has been forgotten or lost to the system.

Procedure

To recover a system administration password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Insert the install tape in the tape drive.
2	Reboot the system from the tape.
3	Select More Utilities from the menu.
4	Select Change to Default System Password. **Result:** You are prompted to enter Yes to continue, or No to stop.
5	Enter Yes to continue. **Result:** The system reports that the operation has been successfully completed. **Result:** This also resets the customer administration password.
6	Remove the install tape from the tape drive.
7	Reboot the system from the disk.
8	Select the [Logon] softkey. **Result:** The system prompts you for a password.
9	Type the default password **adminpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
10	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
11	Type your new password a second time, and press <Return>. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 8 to step 11.

Recovering a customer administration password

Administration level

You can recover the customer administration password from either the System Administration level or the Customer Administration level.

Introduction

This topic describes how to restore a password that has been forgotten or lost to the system.

Procedure

To recover a customer administration password, follow these steps.

Starting Point: Any Menu

Step	Action
1	Insert the install tape in the tape drive.
2	Reboot the system from the tape.
3	Select More Utilities from the menu.
4	Select Change to Default System Password. **Result:** You are prompted to enter Yes to continue, or No to stop.
5	Enter Yes to continue. **Result:** The system reports the operation has been successfully completed. **Result:** This also resets the system administration password.
6	Remove the install tape from the tape drive.
7	Reboot the system from the disk.
8	Select the [Logon] softkey. **Result:** The system prompts you for a password.

Step	Action
9	Type the default password **custpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
10	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
11	Type your new password a second time, and press <Return>. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 8 to step 11.

Logging on from the main administration terminal

Introduction

This topic explains how to log on as the system administrator from the main administration terminal.

Note: If you are logging on from a multiple administration terminal, you cannot perform step 2.

Administration level

The system administrator can access the Customer Administration level from within System Administration.

Procedure

To log on from the main administration terminal, follow these steps.

Starting Point: The Logon/Status screen

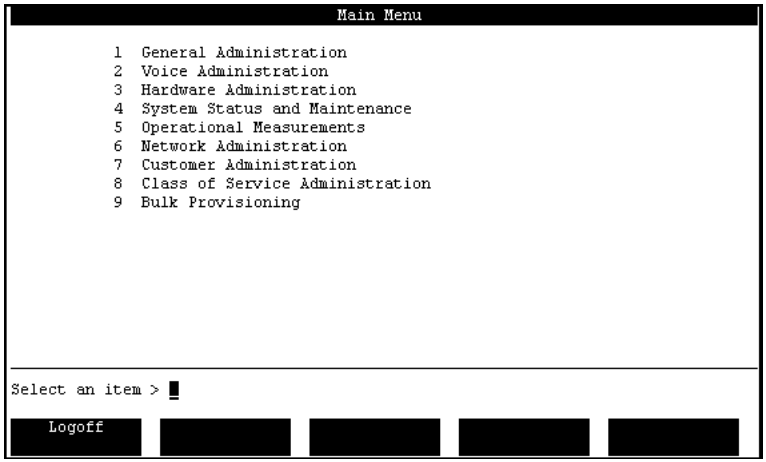
Step	Action
1	Select the [Logon] softkey. **Result:** The system prompts you for a password.
2	Use the following table to determine the next step.

IF	THEN
you are logging on for the first time	see “Setting the system administration password” on page 3-6.
you have logged on before	go to step 3.

3	Type your system administration password, and press <Return>. **Result:** The system displays the Main Menu. **Note:** If an invalid password is entered, an error message appears. Repeat step 1 and step 3.

The Main Menu

The following shows an example of the Main Menu of a multi-customer system displayed at the main administration terminal.



Note: Some of these features may not be available on your system.

ATTENTION

An unsuccessful logon attempt is automatically recorded in the system log file. As a security precaution, after a third unsuccessful attempt to log on, the system forces a 10-minute delay before a further logon attempt is accepted. Only your Nortel representative has the required privileges to gain access to the system during the lockout period.

Logging on from a MAT

Administration level

You can log on from a MAT from the Customer Administration level only.

Introduction

If the Multiple Administration Terminal (MAT) feature is installed on your system, your Meridian Mail system can support up to four administration terminals (one main administration terminal and up to three MATs).

When you are logged on to a secondary terminal, you can perform a limited number of administrative tasks. For more information, see “Types of consoles” on page 3-3.

Your logon password is the same for both the main administration terminal and a MAT.

This topic explains how to log on from a MAT.

The default password

The default password for logging onto a MAT is custpwd.

Changing the default password

The system will prompt you to change the default password the first time you log on. This is for security reasons.

Once you have changed the password after initial logon, you can change the password at any time from the General Administration menu by selecting the Change Customer Administrator Password item.

Restriction
You cannot make the MAT password the same as the system administration password.

Before you begin

The Multiple Administration Terminal feature must be installed on your system.

Logging on from a MAT

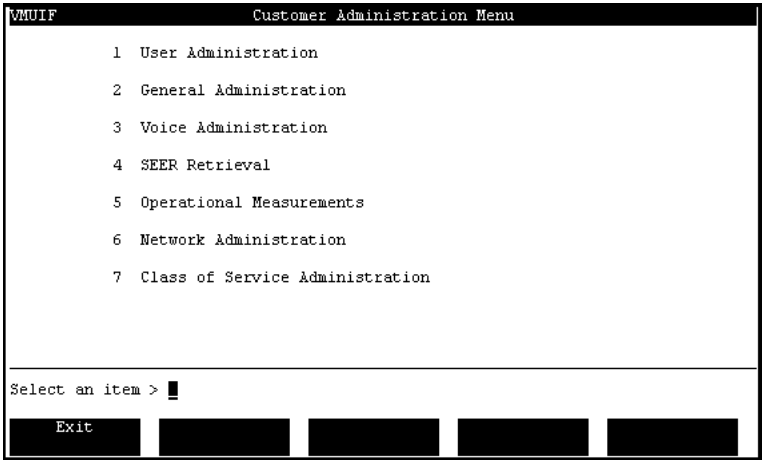
To log on from a MAT, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey.
2	Type the customer administration password, and press <Return>. **Result:** The system displays the Customer Administration Menu. **Note:** If an invalid password is entered, an error message appears. Repeat step 1 and step 2.
3	Press [View/Modify], enter an existing customer number and press <Return>.

The Customer Administration Menu

The following shows an example of the Customer Administration Menu displayed at a MAT.



Logging on from a remote terminal (non-EC system)

Introduction

This topic explains how to log on to the system through a remote terminal from a system that is not a Modular Option EC system.

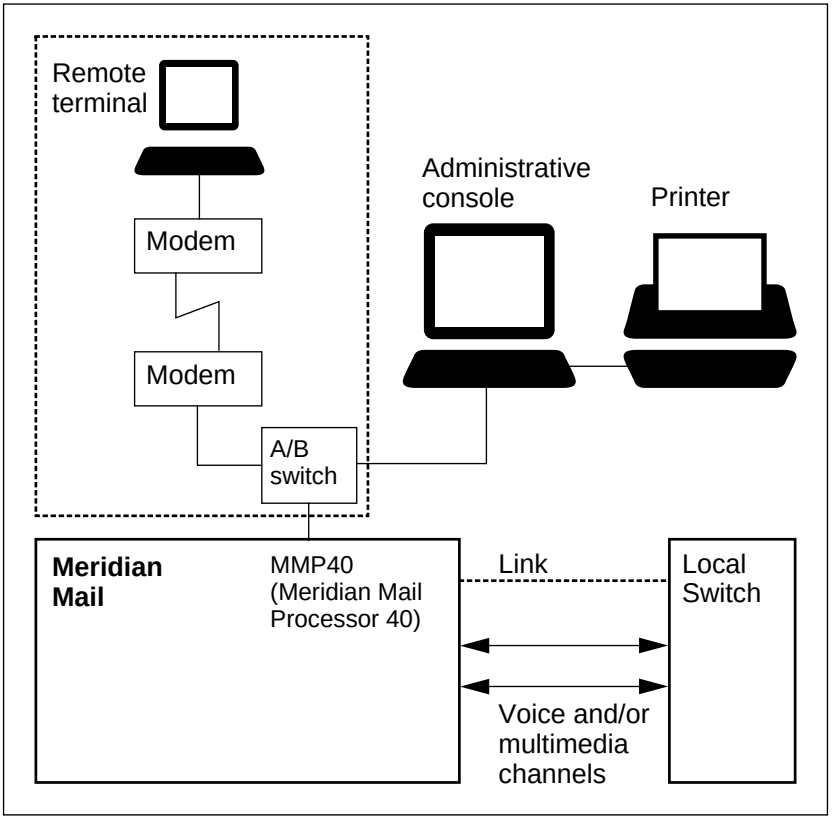
If your installation has a remote administration terminal installed for service personnel, administrative functions can be performed remotely.

Your logon password is the same for both the main administration terminal and the remote terminal.

The administrative functions described in this guide are identical whether viewed from the local administration terminal or from the remote terminal.

Typical remote terminal configuration (non-EC system)

The following diagram shows a typical remote terminal configuration for a system that is not a Modular Option EC system.



Coordinating a remote logon

Because no administrative functions can be carried out from the local console while a remote logon is in effect, a remote logon should be coordinated with the local administrator.

Logging on from a remote terminal (non-EC system)

To log on from a remote terminal on a non-EC system, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	Change the A/B switch setting to remote.
2	Notify the user at the remote terminal. The user at the remote terminal does the following: a. Dial in to the modem. b. Press <Ctrl> <r> to display the Logon screen. c. Type the administration password. d. Carry out administrative tasks as required, and then log off.

Disabling remote terminal access (non-EC system)

To disable remote terminal access on a non-EC system, follow these steps.

Step	Action
1	At the local site, change the A/B switch back to the local setting. **Result:** Control is returned to the local console where the Logon/Status screen is again displayed.

Logging on from a remote terminal (EC system)

Introduction

This topic explains how to log on to the system through a remote terminal on a Modular Option EC system.

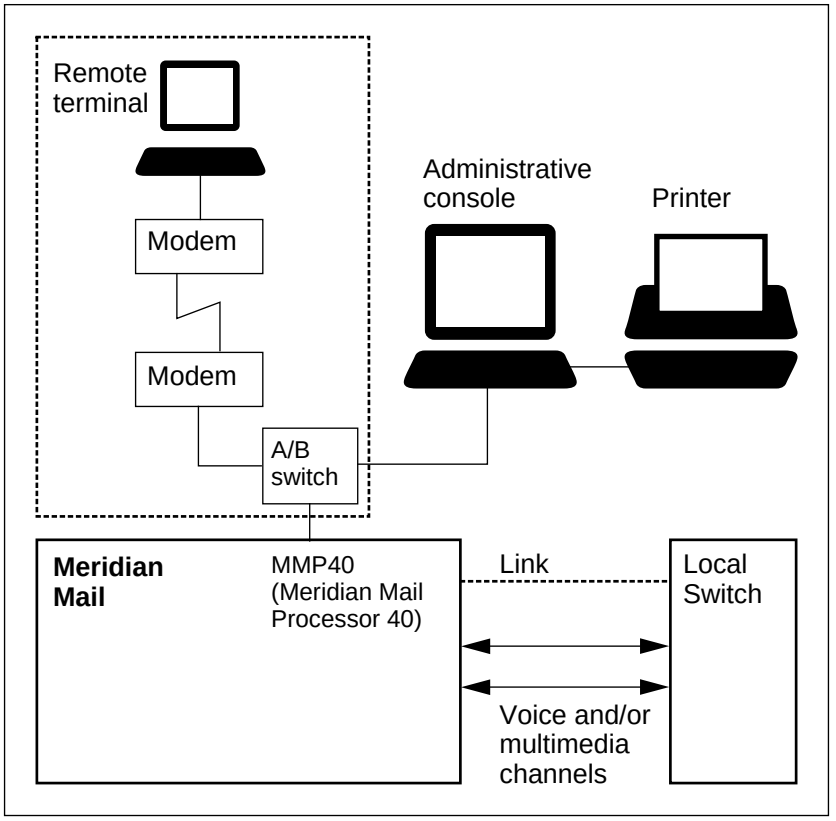
If your installation has a remote administration terminal installed for service personnel, administrative functions can be performed remotely.

Your logon password is the same for both the main administration terminal and the remote terminal.

The administrative functions described in this guide are identical whether viewed from the local administration terminal or from the remote terminal.

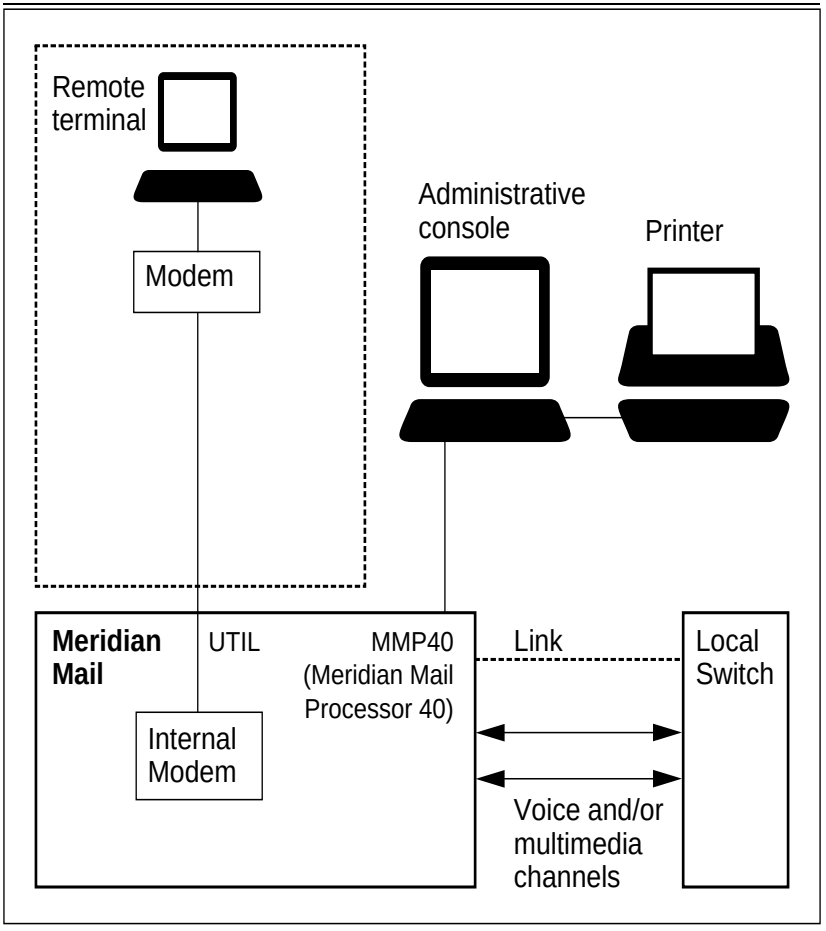
Typical remote terminal configuration (EC system)

The following diagram shows a typical remote terminal configuration for a Modular Option EC system.



Typical remote terminal configuration (EC system with internal modem)

The following diagram shows a typical remote administration configuration with an internal modem on the utility card for a Modular Option EC system.



Coordinating a remote logon

Because no administrative functions can be carried out from the local console while a remote logon is in effect, a remote logon should be coordinated with the local administrator.

Logging on from a remote terminal (EC system)

To log on from a remote terminal on an EC system, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	To bring up the COBRAVT selection window, press <Ctrl> <w>. **Result:** The COBRAVT selection window is displayed. **Note:** For help using COBRAVT, type a question mark (?). A help screen is displayed.
2	Type **m** (case does not matter).
3	Notify the user at the remote terminal.
4	Dial in to the modem. The user at the remote terminal does the following: a. Press the <Break> key to gain control of the console. b. Type the administration password.

Disabling remote terminal access (EC system)

To disable remote terminal access, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	To bring up the COBRAVT selection window, press <Ctrl> <w>. **Result:** The system displays the COBRAVT selection window.
2	Type **m** (case does not matter). **Result:** Control is returned to the local console where the system again displays the Logon/Status screen. **Note:** You can terminate a remote logon at any time if you press <Ctrl> <w> and type **m.**

CAUTION

Risk of data loss

If the remote administrator is in the process of changing system data and a save is not performed before a remote logon is terminated, data may be lost.

Using a single terminal to access the M1 and Meridian Mail

Introduction

If you are logging on at a site with only one terminal access, then you will need to toggle back and forth between the M1 and Meridian Mail.

Procedure

To toggle between the M1 and Meridian Mail, follow these steps.

Step	Action
1	Determine the steps you need to follow. **IF you want to toggle** / **THEN go to** from the M1 to MM / step 2. from MM to the M1 / step 7.
2	Flip the toggle switch to MM.
3	Press <Ctrl> <w> to clear the screen.
4	Press **i**, then **f**.
5	Is the screen displaying the MM interface? If yes, continue. If no, press <Ctrl> <r> to refresh the screen.
6	You can work at the terminal now.
7	Flip the toggle switch to the M1.
8	Press the Setup Key on the keyboard.
9	Use the up and down arrow keys to move to the Clear Display screen, and press <Return>. **Result:** If you are already logged on, the screen displays the M1 prompt: **>** **Result:** If you are not logged on to the M1, the screen displays the prompt:**.**
10	You can work at the terminal now.

Chapter 4

Setting up the system

In this chapter

Overview	4-2
Section A: Basic setup procedures	4-3
Section B: Setting up customers	4-17
Section C: Setting up optional features	4-31

Overview

Introduction

This chapter contains the following information:

- It provides an overview of a complete basic setup of your system.
- It refers you to procedures for checking the provisioning of your Meridian Mail system.
- It lists and describes optional features and refers you to the procedures to set up these features.

Section A: Basic setup procedures

In this section

Overview	4-4
Changing the system administration password	4-5
Checking the hardware configuration	4-6
Checking the system status	4-7
Checking the Channel Allocation Table	4-8
Configuring general system options	4-9
Setting up dialing translations	4-10
Setting up restriction and permission lists	4-11
Defining classes of service	4-12
Configuring operational measurement options	4-13
Configuring optional features and other services	4-14
Setting up system security	4-15
Backing up the system	4-16

Overview

Introduction

This section provides general information and procedures for checking the provisioning of your Meridian Mail system. Wherever necessary, it refers you to more detailed information in other chapters of this guide and in other manuals.

It also provides an overview of a complete basic setup of your system.

Objective

This section is intended as a checklist for system setup.

Before you begin

To ensure that your Meridian Mail system is properly provisioned, refer to the procedures in the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Changing the system administration password

Introduction

This involves logging on to the main administration terminal using the current password, and then following the system instructions to change the password.

You can make password changes only at the main administration terminal. If you have MATs on your system, your changes are then automatically made to them.

Procedure

For information and procedures for changing the system administration password, see Chapter 3, “Logging on”.

Checking the hardware configuration

Introduction

This involves checking the node configuration and the data port configuration.

Check the data port configuration to verify the assignment of data devices, especially parameters such as the baud rate and parity for the administration console.

Procedure

To check the hardware configuration, refer to the procedures in the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Checking the system status

Introduction

This involves verifying the status of the system and enabling or disabling system nodes and DSP ports.

Procedure

For information and procedures for checking the system status, see Chapter 29, “System status and maintenance”.

Checking the Channel Allocation Table

Introduction

This involves configuring the primary DN and Channel DN for each agent/channel. It also involves configuring the service or services for which the channel will be used. In most cases, channels are shared by all services. If any channels are to be dedicated to a specific service, enter the service in the Channel Allocation Table.

You check the Channel Allocation Table to ensure consistency between the switch and the Meridian Mail system.

Note: This step should be carried out only by a qualified technician.

Procedure

To check the Channel Allocation Table, see “Channel Allocation Table” on page 29-45.

Configuring general system options

Introduction

This involves viewing the features that are installed on your system and configuring the attendant DN and date format for reports. The General Options screen is also where you assign classes of service to the system. You can also modify the SEER and Reports printer port names if different from the console port.

Procedure

For information and procedures for configuring general system options, see Chapter 14, “General options”.

Setting up dialing translations

Introduction

This involves defining network access prefixes for local off-switch, long distance, and international dialing, and for dialing translation tables.

Procedure

For information and procedures for setting up dialing translations, see Chapter 18, “Dialing translations”.

Setting up restriction and permission lists

Introduction

This involves modifying the restriction and permission codes to allow users to dial only the external phone numbers or internal extension numbers that you specify. Unless you are upgrading from an earlier release of Meridian Mail, features such as Mailbox Thru-Dial, Custom Revert DN, or Extension Dialing are initially restricted and do not work until you modify the restriction and permission codes.

You define restriction and permission codes to prevent external callers or internal users from placing local or long distance calls that you do not want billed to your system.

Note: This is a very important step.

Procedure

For information and procedures for setting up restriction and permission lists, see Chapter 7, “Setting up Meridian Mail security”.

Defining classes of service

Introduction

This involves identifying which of your users have similar needs and what those needs are, and then defining the operating parameters or Class of Service (COS) for each group of users.

When you change a parameter in a COS, all users belonging to that COS have the changes automatically updated.

> **ATTENTION**
>
> You must add classes of service before you add users. Each user must be assigned to a class of service.

Procedure

For information and procedures for defining classes of service, see Chapter 27, “Class of Service administration”.

Assigning COSs to the system

After you add classes of service you must assign them to the system. If you do not do this, the classes of service will not show up in the Add a Local Voice User screen and you will not be able to assign them to users.

Classes of service are assigned to the system in the General Options screen.

Configuring operational measurement options

Introduction

This involves defining how system and user statistics are collected. This includes, for example, the kinds of data to be collected, the time that traffic data collection begins and ends each day, and how often collected traffic statistics are written to disk.

You do not need to configure the operational measurement options right away. You may choose instead to use the default settings.

You can then modify these settings after your system has been in use for a time to provide a level of detail that is more appropriate for your needs.

Procedure

For information and procedures for configuring operational measurement options, see Chapter 31, “Operational Measurements”.

Configuring optional features and other services

Introduction

This involves configuring optional features that are installed on your system, such as Fax on Demand or AMIS Networking.

You can either continue with the configuration of these optional features or back up the system now and continue at a later time.

Procedure

For information and procedures for configuring optional features and other services, see “Setting up optional features” on page 4-31.

Setting up system security

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. It is necessary to take all possible precautions to prevent security breaches.

If your system is properly secured, it is difficult for a user connected to Meridian Mail (such as a user who is logged on to a mailbox or an external caller who has connected to Meridian Mail through a call answering session or a voice menu) to place unauthorized calls that will be billed to your system.

Procedure

For information and procedures for setting up system security, see Chapter 7, "Setting up Meridian Mail security".

Backing up the system

Introduction

After you have finished customizing your system configuration, back up the new data onto tape to ensure its safety. This involves making backup copies of some or all of the system's data.

In the event of disk failure, you will not need to reenter user and site-specific information, and you can bring your system back into service quickly.

Procedure

For information and procedures for backing up the system, see Chapter 16, "Back up and restore Meridian Mail data".

Section B: Setting up customers

In this section

Overview	4-18
Changing the customer administration password	4-19
Adding customers to the system	4-20
Enabling features for each customer	4-21
Assigning classes of service to each customer	4-22
Setting the attendant DN for each customer	4-23
Customizing voice messaging options for each customer	4-24
Customizing voice security options for each customer	4-25
Adding voice service DNs	4-26
Adding users to customers	4-27
Creating distribution lists	4-28
Configuring optional features and other services	4-29
Backing up the system from the system administration level	4-30

Overview

Administration level

This section applies to an administrator at the Customer Administration level only.

Introduction

Once you have configured the basic system parameters, you are ready to add customer groups, configure them to meet the requirements of your customers, and add users.

Most of the optional features that can be installed on Meridian Mail also require configuration at the customer administration level.

This section outlines general procedures and provides references that explain the various aspects of configuration in more detail.

Changing the customer administration password

Introduction

This involves logging on to the main administration terminal using the current password and then following the system instructions to change the password.

You can make password changes only at the main administration terminal. If you have MATs on your system, your changes are then automatically made to them.

Procedure

For information and procedures for changing the customer administration password, see Chapter 3, “Logging on”.

Adding customers to the system

Introduction

This step must be done before you add users. It involves logging on, and adding a specified customer from the Customer Administration screen

Procedure

For information and procedures for adding customers to the system, see Chapter 5, “Customer administration”.

Enabling features for each customer

Introduction

You must enable any of the following features, if they are on your system, for each customer. Each feature is disabled by default for all customers.

The features include

- Voice Menus and Announcements (if installed)
- Voice Forms (if installed)
- Meridian Mail Networking (if installed)
- Fax on Demand (if installed)

Procedure

For information and procedures to enable features, see Chapter 14, “General options”.

Assigning classes of service to each customer

Introduction

You need to assign a class of service to each customer. Up to 15 of 127 possible classes of service are available. Your choice of possible classes of service for users depends upon which classes of service were previously assigned to the customer.

You can only assign those classes of service to users of a customer that have already been assigned to that customer.

Procedure

For information and procedures to assign a class of service to each customer, see Chapter 14, “General options”.

Setting the attendant DN for each customer

Introduction

If Meridian Mail is unable to handle a call, it is reverted back to an assigned number, the Attendant DN. Each user may have a custom revert DN, but the number you enter here is used as the default when adding users.

Note: An attendant DN cannot be configured if VMUIF is enabled for the customer.

Procedure

For information and procedures to set the attendant DN for each customer, see Chapter 14, “General options”.

Customizing voice messaging options for each customer

Introduction

You may assign certain voice messaging options to the customer.

The options for MMUI customers include

- recording a custom call answering greeting
- configuring the broadcast mailbox number
- enabling users to record their own personal verifications (if desired)
- setting the maximum messaging length
- setting the maximum amount of time that a user's read messages are kept before being deleted by the system
- (if your system is multilingual), selecting the default language and secondary default language
- enabling speed control, to permit mailbox users to control message playback speed

The options for VMUIF customers include

- recording a customized VMUIF introductory tutorial
- configuring the lockout revert DN
- configuring the maximum message length
- configuring the maximum amount of time that a user's read messages are kept before being deleted by the system

Procedure

For more information on voice messaging options, see Chapter 21, "Voice messaging options".

Customizing voice security options for each customer

Introduction

In order to protect your system from abuse, you can

- limit the number of invalid logon attempts before users are locked out of their mailbox
- change the default parameters that require users to update their passwords
- define the password prefix to be used when generating passwords for newly created mailboxes

Procedure

For detailed information on security, see Chapter 7, “Setting up Meridian Mail security”.

Adding voice service DNs

Introduction

For each voice service that you can dial directly by internal users or external callers, you must define a DN in the VSDN table. This includes services such as voice messaging and express messaging.

Procedure

To add voice service DNs, see “The VSDN table” on page 25-9.

Adding users to customers

Introduction

Before adding users to a customer, you should consider the following:

- Read “Distributing local voice users evenly over volumes” on page 8-17.
- Before adding users, determine which users should be assigned to which classes of service.

Procedure

Once you determine the needs of your users, you can choose from the following procedures.

WHEN you want to	THEN
add local voice users	see Chapter 9, “Local voice users”.
add directory entry users	see Chapter 11, “Directory entry users”.
add users at remote sites (if Networking is installed)	see Chapter 10, “Remote voice users”.

Creating distribution lists

Introduction

A distribution list is a collection of mailbox numbers. It allows you to send the same message to a number of people. Distribution lists are convenient if you frequently have to send messages to the same group or groups of people (within the customer.)

You do not need to create customer distribution lists as part of the initial configuration. If you know which lists you need, then you can create them, but they can be created at any time.

Procedure

For information and procedures for creating distribution lists, see Chapter 12, “Distribution lists”.

Configuring optional features and other services

Introduction

You may continue to configure your system or perform a system backup. Either follow “Backing up the system from the system administration level” on page 4-30, or consider the following.

Procedure

To configure any of these optional features on your system, refer to the following NTPs:

- *Voice Services Application Guide* (NTP 555-7001-325)
- *Fax on Demand Application Guide* (NTP 555-7001-327)
- *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242)
- *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244)
- *Meridian Mail Enterprise Networking Installation and Administration Guide* (NTP 555-7001-246)

You can find individual optional features and other services in Section C: Setting up optional features.

Backing up the system from the system administration level

Introduction

Once you have customized the system configuration, you should back up the data to ensure its safety from the system administrator level.

Procedure

See “Backing up the system” on page 4-16 after you exit the Customer Administration level.

Section C: Setting up optional features

In this section

Overview	4-32
Setting up the Outcalling feature	4-33
Setting up the Voice Menus feature	4-34
Setting up the Voice Forms feature	4-35
Setting up the Fax on Demand feature	4-36
Setting up the Meridian Networking feature	4-37
Setting up the AMIS Networking feature	4-38
Setting up the Virtual Node AMIS Networking feature	4-39
Setting up the Enterprise Networking feature	4-40
Setting up the Hospitality feature	4-41
Setting up the Meridian Mail Reporter feature	4-42
Setting up the Meridian Mail AutoAdmin feature	4-43
Setting up the ACCESS feature	4-44

Overview

Introduction

This section introduces the following optional features:

- Outcalling
- Voice Menus
- Voice Forms
- Fax on Demand
- Meridian Mail Networking (includes Meridian and Enterprise Networking)
- AMIS Networking
- Hospitality
- Meridian Mail Reporter
- Meridian Mail AutoAdmin
- ACCESS

It also refers you to the procedures and information you require to set up these features.

Setting up the Outcalling feature

Introduction

The Outcalling feature refers to two functions: the Remote Notification feature and the Delivery to Non-User feature.

Remote Notification allows Meridian Mail users to be notified of new messages at remote phone or pager numbers. Delivery to Non-User allows users to compose and send messages to people outside the Meridian Mail system.

Procedure

For information and procedures for setting up the Outcalling feature, refer to *Meridian Mail Outcalling Application Guide* (NTP 555-7001-320).

Setting up the Voice Menus feature

Introduction

The Voice Menus feature enables you to create a number of custom call answering applications.

The Announcements service allows you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly.

Thru-Dial services access predefined DNs or user-prompted DNs that can be used either within a voice menu service or as a separate service with a directory number. Thru-Dial services can be set up to allow Name Dialing and can have restrictions barring users from dialing unauthorized numbers, such as long distance access codes.

The Time-of-Day Controllers service allows you to control the activation of voice services based on the date and time at which a call is received. This allows you to control the availability of voice services during off-hours and holidays.

The Voice Menus service enables you to create single-layered or multilayered menus that present callers with a series of choices about the action they can perform.

The Voice Prompt Maintenance service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

The Remote Activation service allows you to enable or disable voice services while you are offsite through a standard dual-tone multifrequency (touch tone) telephone set.

Procedure

For information and procedures for setting up the Voice Menus feature, refer to *Meridian Mail Voice Services Application Guide* (NTP 555-7001-325).

Setting up the Voice Forms feature

Introduction

The Voice Forms feature has two parts: Voice Forms administration and Voice Forms transcription.

Voice Forms administration involves the creation of applications that collect voice information from callers. An application consists of a series of questions, played in sequential order, to which callers give voice responses. It is as if callers are filling in a form over the phone.

Voice Forms transcription refers to the process of retrieving the information collected by a voice form application. Once retrieved, the data can be processed in a number of ways, depending on why you have collected the information.

Procedure

For information and procedures for setting up the Voice Forms feature, refer to *Meridian Mail Voice Services Application Guide* (NTP 555-7001-325).

Setting up the Fax on Demand feature

Introduction

Fax on Demand is a Meridian Mail feature that allows a caller to obtain information in the form of a fax. The fax information is stored in Meridian Mail and is sent on request to a fax device.

The configuration of the Fax on Demand application affects its available features. For example, fax documents may be stored either as stand-alone, directly dialed fax items, or as items selected from voice menus. Depending on how the Fax on Demand application is configured and on whether the caller is using a fax phone, fax information may be delivered as part of the call requesting the information, or later, by callback to the caller's fax device.

Procedure

For information and procedures for setting up the Fax on Demand feature, refer to *Meridian Mail Fax on Demand Application Guide* (NTP 555-7001-327).

Setting up the Meridian Networking feature

Introduction

Meridian Networking is a Meridian Mail networking protocol that permits one or more Meridian Mail systems to send messages to and receive messages from users at remote Meridian Mail sites.

It uses the following:

- a network database to define local and remote sites
- a hybrid analog and digital transmission scheme
- modems to transmit control passwords, message header information, and message delivery acknowledgments between sites

Procedure

For information and procedures for setting up the Meridian Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Setting up the AMIS Networking feature

Introduction

AMIS Networking uses the Audio Messaging Interface Specification (AMIS) protocol. This protocol permits users to send messages to and receive messages from users at other voice messaging systems that also use the AMIS protocol (not necessarily Meridian Mail systems).

AMIS does not require special hardware or passwords. It does, however, require the ability to generate dual-tone multifrequency (DTMF) tones.

Procedure

For information and procedures for setting up the AMIS Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242).

Setting up the Virtual Node AMIS Networking feature

Introduction

Virtual Node AMIS Networking is a combination of Meridian Networking and AMIS Networking. Meridian Networking provide the ability to define local and remote sites as using the AMIS protocol. Sites that use the AMIS protocol are called virtual nodes. They may or may not have a Meridian Mail system installed.

Virtual Node AMIS uses the AMIS protocol to deliver messages. As a result, Virtual Node AMIS messages are restricted to the same functionality as the AMIS protocol.

Procedure

For information and procedures for setting up the Virtual Node AMIS Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245).

Setting up the Enterprise Networking feature

Introduction

Enterprise Networking is a Meridian Mail Networking protocol that permits one or more Meridian Mail systems to send messages to and receive messages from users at remote Meridian Mail sites. It uses the following:

- a network database to define local and remote sites
- DTMF signaling based on the AMIS protocol, instead of modems, to transmit messages between sites

Procedure

For information and procedures for setting up the Enterprise Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Enterprise Networking Installation and Administration Guide* (NTP 555-7001-246).

Setting up the Hospitality feature

Introduction

The Meridian Hospitality Voice Service (MHVS) provides specialized functions for the hotel industry. The MHVS system consists of Meridian 1/SL-1 and Meridian Mail components connected to a Property Management System. MHVS provides voice messaging services to hotel staff and guests and automates the management of mailboxes for guest rooms.

When a guest checks in to the hotel, a mailbox is created for the room the guest will be occupying. Upon checkout, the mailbox is removed, and any read or unread messages that arrived for that guest prior to checkout are moved to a post-checkout mailbox for later retrieval.

Procedure

For information and procedures for setting up the Hospitality feature, refer to the *Hospitality Voice Services Implementation Guide* (NTP 555-7001-221).

Setting up the Meridian Mail Reporter feature

Introduction

Meridian Mail Reporter is an application that runs on a PC connected to Meridian Mail and enables you to download operational measurements data. Using this information, you can produce and print summary and detailed reports for use in managing Meridian Mail systems.

These reports support all areas of administrative responsibility, including general administration, troubleshooting, security, capacity analysis, and billing.

Procedure

For information and procedures for setting up the Meridian Mail Reporter feature, refer to the *Meridian Mail Reporter User's Guide* (P019082).

Setting up the Meridian Mail AutoAdmin feature

Introduction

Meridian Mail AutoAdmin is an application that runs on a PC connected to Meridian Mail; through it you can add, view, update, and delete user mailboxes. AutoAdmin allows large messaging customers such as universities, hospitals, government entities, and so on, to mass-create mailboxes with user data entered in another system and transferred to AutoAdmin, thereby reducing errors and data entry effort.

Procedure

For instructions on setting up and using AutoAdmin, see Appendix B, “Meridian Mail AutoAdmin Utility”, in this manual.

Setting up the ACCESS feature

Introduction

ACCESS uses a Unix interface to provide a development tool for creating specialized voice service applications for incoming or outgoing calls or for administrative purposes.

ACCESS applications can make use of the full range of voice and telephony functions that a digital voice processing system and a telephone switching system can offer. No special voice or telephone interface cards are needed, as the PBX and Meridian Mail together provide all of the necessary resources.

An ACCESS application can receive or place telephone calls, play prompts, receive "input" in the form of keypresses on a touch tone phone keypad (which can be interpreted as commands or data), transfer calls, record messages, and use Meridian Mail services.

Examples of ACCESS applications include banking-by-phone and order entry-by-phone, where the system places orders for callers based on the caller input on a touch tone telephone.

Procedure

For information and procedures for setting up the ACCESS feature, refer to the following publications:

- *Meridian ACCESS Configuration Guide* (NTP 555-7001-315)
- *Meridian ACCESS Developer's Guide* (NTP 555-7001-316)
- *Meridian ACCESS Voice Prompt Editor User's Guide* (NTP 555-7001-318)

Chapter 5

Customer administration

In this chapter

Overview	5-2
New installations	5-3
Adding customers	5-4
Provisioning customers	5-9
Finding, listing, and printing customers	5-11
Selecting a customer to view or modify	5-17
Deleting customers	5-22

Overview

Introduction

Before you can begin adding users to your system, you must add customers. All users must be added to a particular customer.

In this chapter

This chapter describes how to

- add customers
- find existing customers
- list or print all customers, or a subset of customers
- view or modify existing customers
- delete customers

Provisioning customers

Once you have added customers, you are ready to provision them by

- defining customer-specific general options
- adding VSDNs to the VSDN Table for each customer
- adding users to each customer
- creating the necessary voice and fax services for each customer

This is described in more detail in “Provisioning customers” on page 5-9.

Nightly audits

Do not add customers during the nightly audit.

ATTENTION

Do not add, modify, or delete customers during the nightly audit that begins at 3:30 a.m. This audit can take anywhere from 10 minutes to approximately 3 hours.

New installations

Default customer

When Meridian Mail is installed, one default customer is automatically added to the system.

This customer is numbered as customer 1.

You can either

- Leave this default customer as is (do not use it) and add your own customers.
- Modify Customer 1 and use it as one of your customers.

  To do this you must
  - Change the customer's name in the General Options screen.
  - Follow the procedure to modify a customer on page 5-17.

Selecting a method

You can add customers to your system in one of two ways.

Method 1

Add all customers to the system first and then modify each customer in order to configure customer-specific parameters.

Method 2

Add a customer and then configure all of the necessary parameters. Add the next customer, and configure all customer-specific parameters for that customer. Continue in this way until all customers have been added and configured.

Adding customers

When to use

Follow this procedure to add customers to a newly installed system, or to add additional customers to an operational system.

MATs

If the Multiple Administration Terminals (MAT) feature is installed, you must log on from the primary terminal to add customers. You cannot add customers from a secondary terminal.

The Add Customer screen

Customers are added using the Add Customer screen.

Field descriptions

This table describes the fields in the Add Customer screen.

Customer Number	
Description	This is the number of the customer.
Default	The number you entered to access this screen (after pressing [Add]).
Valid range	1 to 2000

Customer Name	
Description	The name of the customer.
Default	Blank
Maximum length	30 characters

Customer Type	
Description	This is the type of customer.
Default	Private
Valid options	Private, Residential, Hospitality • ***Private*** is intended for centrex customers. • ***Residential*** is intended for residential customers. When this option is selected, users do not have access to name dialing or name addressing, even if the interface type is MMUI. • ***Hospitality*** is intended for the hospitality (hotel) industry. This option can only be selected for one customer, since Hospitality can only be enabled for one customer.

Interface Type	
Description	This is the voice messaging interface that will be enabled for telset users belonging to the customer.
Default	MMUI
Valid options	MMUI, VMUIF (one or both interfaces may be installed on your system) • ***MMUI*** provides users with a command-driven telset interface. It is for users who require call answering and voice messaging capabilities (typically Private customers). • ***VMUIF*** provides a menu-driven telset interface. It is primarily for users who need call answering capability only (typically Residential customers). However, compose capability can be enabled for VMUIF users.
See also	For more information, see “Meridian Mail telset interfaces” on page 2-60.

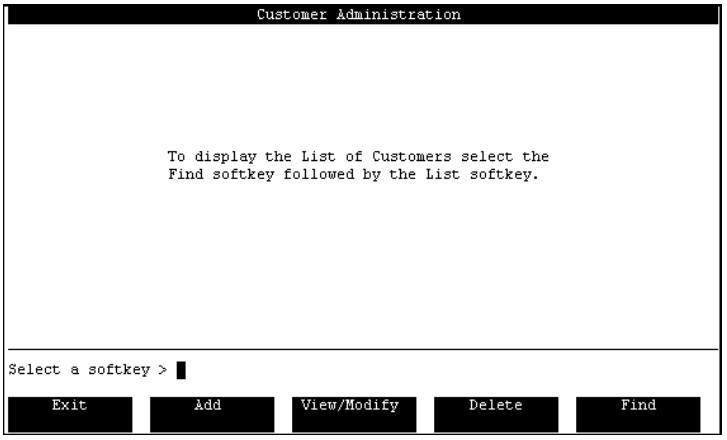
Procedure

This procedure assumes that the system administration password is used to log on. If you log on with the customer administration password, the softkeys shown in Step 1 are immediately displayed. In this case, the [Exit] softkey is replaced with the [Logoff] softkey.

To add a customer, follow these steps.

Starting Point: The Main Menu

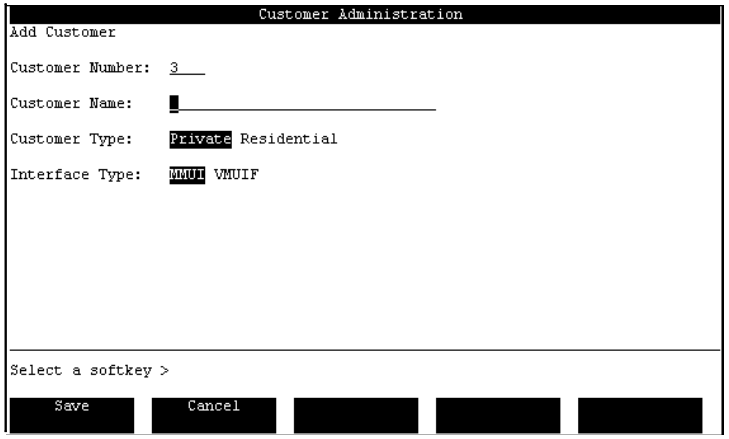
Step	Action
1	Select Customer Administration. **Result:** The Customer Administration screen and softkeys are displayed.



Note: If you logged on from a secondary (MAT) terminal, the [Add] and [Delete] softkeys are not displayed.

2 Press the [Add] softkey.
Result: You are prompted for a customer number.

Step	Action
3	Enter a customer number (between 1 and 2000) and press Return. **Result:** The Add Customer screen is displayed.



4 Enter the customer name.

5 Select the customer type.

IF	THEN choose
you are adding a centrex customer or you want users to have access to name dialing and name addressing, or both	Private.
are adding a residential customer or you do not want users to have access to name dialing and name addressing, or both	Residential.
Hospitality Voice Messaging will be enabled for the customer	Hospitality.

Step	Action

6 Select the interface type.

IF the customer needs any of the following	THEN choose
• Hospitality • Full-featured Voice Messaging • Meridian Networking • Virtual Node AMIS Networking • Express Messaging • Name Addressing/Name Dialing • Dual Language Prompting • User-changeable RN schedules	MMUI.
• Call Answering only • Submailboxes • Rotary telset interface	VMUIF.

Note: For a complete list of features supported by each interface, see “Meridian Mail telset interfaces” on page 2-60.

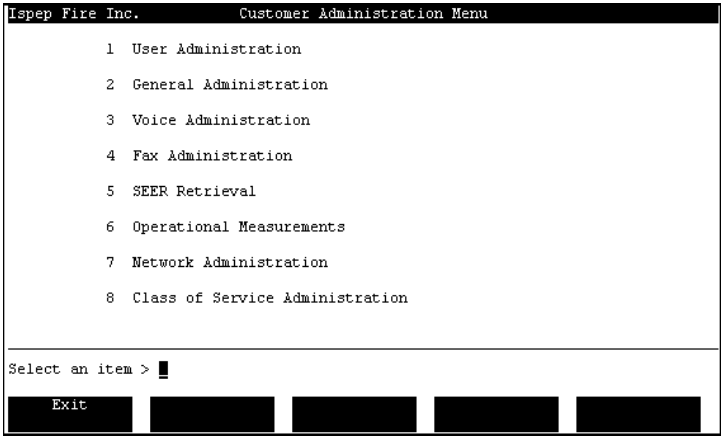
7 Do you want to save the customer with the information you have entered?

- If yes, go to step 8.
- If no, press the [Cancel] softkey.

  Result: The Customer Administration softkeys are displayed.

8 Press the [Save] softkey.

Result: The Customer Administration menu is displayed.



Provisioning customers

Introduction Once you have added a customer to the system, you are ready to add users to it and define customer-specific parameters.

Procedure To provision a customer, follow these steps.

Step	Action	See
1	Enable optional features. These include • Voice Menus and Announcements • Voice Forms • Fax on Demand • Networking	Chapter 14: General options
2	Assign up to 15 classes of service (COSs) to each customer. COSs must already be configured.	Chapter 14: General options
3	Set the attendant DN.	Chapter 14: General options
4	Add a VSDN for each dialable service that is required by the customer.	Chapter 24: Configuring Meridian Mail services Chapter 25: The VSDN table
5	Customize voice messaging options. This involves • setting up languages if more than one language is installed • customizing recordings such as the (MMUI) call answering greeting and VMUIF tutorials • setting up operational characteristics for voice messaging	Chapter 21: Voice messaging options
6	Customize voice security options. This includes • defining a password prefix • setting the maximum number of invalid logon attempts • making mailbox passwords as secure as possible	Chapter 7: Setting up Meridian Mail security
7	If Networking is installed and enabled for the customer, configuring Meridian Networking.	the appropriate Networking Guides
8	Add local voice users (mailboxes).	Chapter 9: Local voice users
9	Add directory entry users (if necessary).	Chapter 11: Directory entry users

Step	Action	See
10	If Meridian Networking is enabled for the customer, add remote voice users to that customer.	Chapter 10: Remote voice users
11	Create the necessary distribution lists for each customer.	Chapter 12: Distribution lists
12	If Voice Menus and Announcements are enabled, create the necessary voice services (voice menus, announcements, time-of-day controllers, thru-dialers) for the customer.	the *Voice Menus Application Guide*
13	If Voice Forms are enabled, create the necessary voice forms for the customer.	the *Voice Forms Application Guide*
14	If Fax on Demand is enabled, create the necessary fax items and set up the fax item maintenance service for the customer.	the *Fax on Demand Application Guide*

After setting up customers

Once you have finished setting up customers, be sure to back up the system to save your configuration.

See Chapter 16, “Back up and restore Meridian Mail data. ”

Finding, listing, and printing customers

When to use

Use the find function if you want to

- find and list all or a subset of customers on screen
- find and print a list of all or a subset of customers
- find a particular customer when you do not know the customer number (so that you can view, modify, or delete the customer)

The Find Customer screen

Search criteria are specified in the Find Customer screen.

The list format

The List Format field determines the information that is displayed in the list of found customers.

The default is Brief.

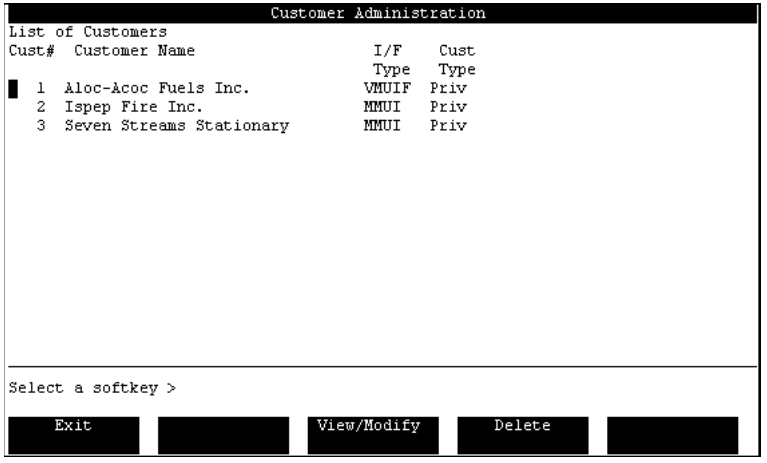
Your options are Brief, Attribute, and COS.

Brief

When you select Brief, the customer number and customer name are displayed.

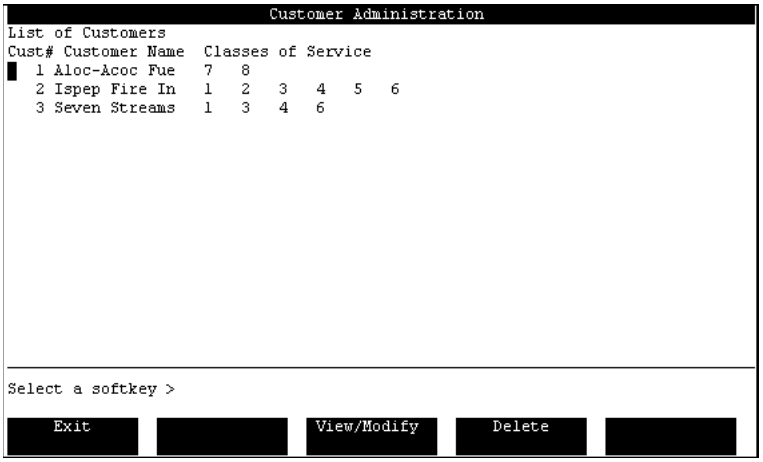
Attribute

When you select Attribute, the customer number, customer name, interface type, and customer type are displayed.



COS

When you select COS, the customer number, customer name, and the classes of service assigned to each customer are displayed.


Customer Administration
List of Customers
Cust# Customer Name Classes of Service
1 Aloc-Acoc Fue 7 8
2 Ispep Fire In 1 2 3 4 5 6
3 Seven Streams 1 3 4 6
Select a softkey >
Exit
View/Modify
Delete

Wildcards

There are two wildcard characters that you can use in the Customer Number and Customer Name fields.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.

Examples

Here are some of examples of how you can use wildcards.

You enter	Result
“2_” in the Customer Number field	Customers in the range 20 to 29 are found.
“2+” in the Customer Number field	Customers beginning with 2 are found (20 to 29, 200 to 299, 2000).
“+Engineering” in the Customer Name field	Customers whose names end with the word Engineering are found, such as Hardware Engineering and Software Engineering.

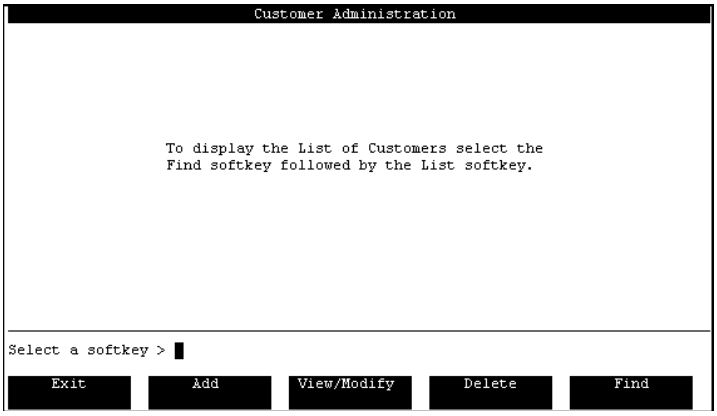
Procedure

This procedure assumes that the system administration password is used to log on. If you log on with the customer administration password, the softkeys shown in Step 1 are immediately displayed. In this case, the [Exit] softkey is replaced with the [Logoff] softkey.

To find a customer (or customers), follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Customer Administration. **Result:** The Customer Administration screen and softkeys are displayed.



2	Press the [Find] softkey. **Result:** The Find Customer screen is displayed.

Step	Action
3	Select the format in which you want found customers to be displayed or printed in the List Format field.
4	Do you want to find a subset of customers within a range of customer numbers? • If yes, enter the necessary number(s) and wildcard(s) to specify the range and go to step 6. • If no, go to step 5.
5	Enter the name of the customer you want to find. **Note:** You can use wildcards in this field if you are unsure of the spelling or if you want to find customers that are similarly named.
6	List or print the found customers.

IF you want to	THEN
list the found customers on screen	go to step 7.
print the list of found customers	go to step 9.

7 Press the [List] softkey.

Result: The List of Customers screen is displayed.

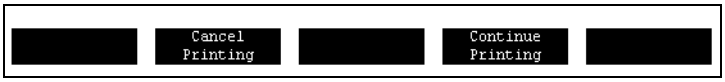
Note: The [Delete] softkey is not displayed if you have logged on from a secondary terminal, or if there is only one customer.

Step	Action
8	You can do one of the following.

IF you want to	THEN
view or modify one or more of the found customers	see page 5-17.
delete one or more of the found customers	see page 5-22.
leave the List of Customers screen	press [Exit].

9 Press the [Print] softkey.

Result: The printing softkeys are displayed.



10 Do you want to continue?

- If yes, make sure the printer has paper and press the [Continue Printing] softkey.

  Note: You can press [Cancel Printing] once printing has started in order to stop.
- If no, press the [Cancel Printing] softkey.

Selecting a customer to view or modify

When to use

Use this procedure when you want to view or modify a customer.

Before you view or modify a customer's setup, you must select one of the existing customers to make it the current customer. When you select a particular customer, all of the screens you view or modify are specific to that customer.

Choosing a procedure

You may or may not know the number of the customer you want to view or modify. Use this table to decide which procedure to follow.

IF	THEN follow
you know the customer number	"Selecting a customer when you know the customer number" on page 5-18.
you do not know the customer number	"Selecting a customer when you do not know the customer number" on page 5-20.

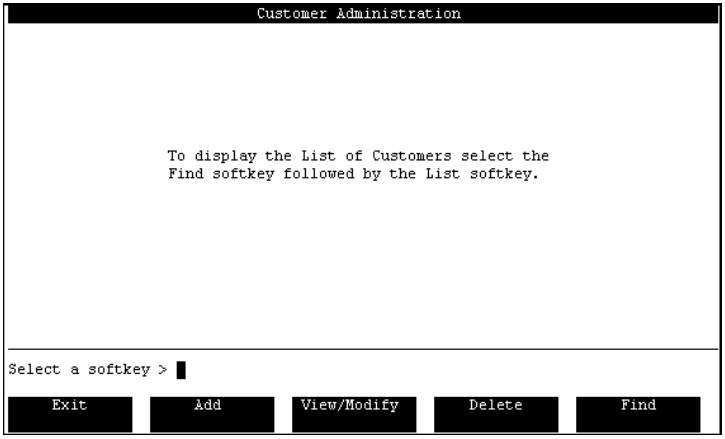
Selecting a customer when you know the customer number

This procedure assumes that the system administration password is used to log on. If you log on with the customer administration password, the softkeys shown in Step 1 are immediately displayed. In this case, the [Exit] softkey is replaced with the [Logoff] softkey.

To view or modify a customer when you know the customer number, follow these steps.

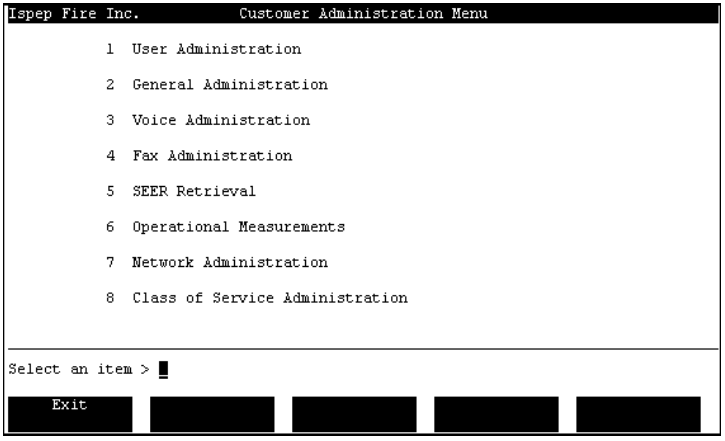
Starting Point: The Main Menu

Step	Action
1	Select Customer Administration. **Result:** The Customer Administration screen and softkeys are displayed.



2	Press the [View/Modify] softkey. **Result:** You are prompted for the customer number.

Step	Action
3	Enter the number of the customer you want to view or modify and press Return. **Result:** The Customer Administration Menu is displayed.



Note: If you have logged on from a secondary terminal, only the following items are displayed: User Administration, Voice Services Administration, and Class of Service Administration.

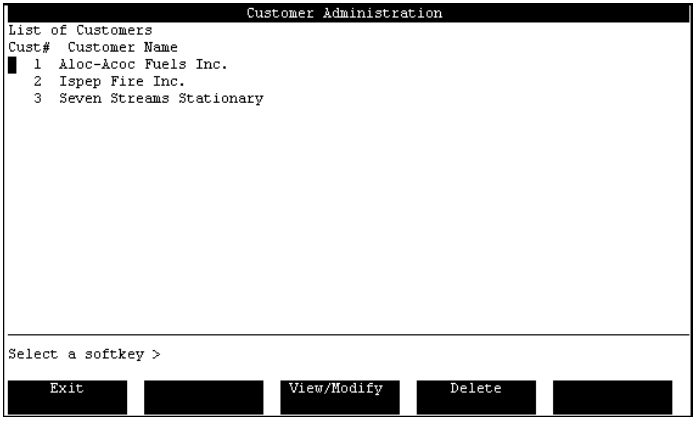
4 Select the menu item that corresponds to the activity you want to perform and press Return. See the appropriate chapter or document for further instructions.

Selecting a customer when you do not know the customer number

If you do not know the number of the customer you want to view or modify, follow these steps.

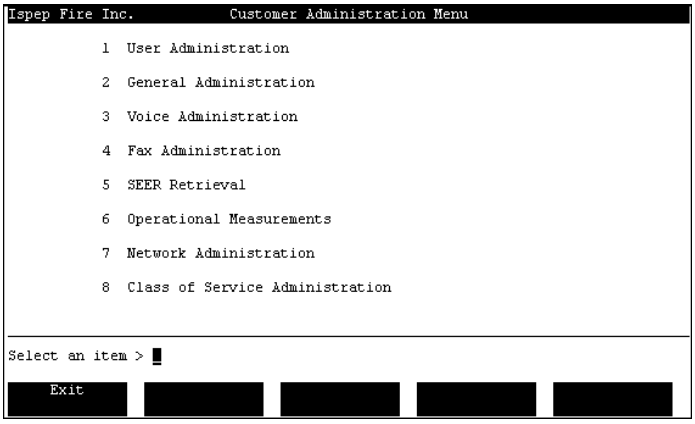
Starting Point: The Main Menu

Step	Action
1	Follow the procedure for finding customers on page 5-14 and then return to this procedure. **Note:** Use the [List] softkey to get a list of customers.



2	Select the customer you want to view or modify by putting the cursor on that customer and pressing the space bar.

Step	Action
3	Press the [View/Modify] softkey. **Result:** The Customer Administration Menu for the selected customer is displayed.



Note: If you have logged on from a secondary terminal, only the following items are displayed: User Administration, Voice Services Administration, and Class of Service Administration.

4 Select the menu item that corresponds to the activity you want to perform and press Return. See the appropriate chapter or document for further instructions.

Deleting customers

When to use

Use this procedure if a customer is no longer required and needs to be deleted from the system.

Restrictions

You cannot delete customers if

- you have logged on from a secondary (MAT) terminal
- there is only one customer

Before you begin

If you try to delete a customer that still has users and services associated with it, you will not be able to delete it. You must, therefore, delete the following before you can delete a customer:

- all users that have been added to the customer
- all voice and fax services that have been created for the customer
- all VSDNs that have been created for the customer

Choosing a procedure

You may or may not know the number of the customer you want to delete. Use this table to decide which procedure to follow.

IF	THEN follow
you know the customer number	“Deleting a customer when you know the customer number” on page 5-23.
you do not know the customer number	“Deleting a customer when you do not know the customer number” on page 5-25.

Deleting a customer when you know the customer number

To delete a customer when you know the customer number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Customer Administration. **Result:** The Customer Administration screen and softkeys are displayed.

Note: The [Delete] softkey is not displayed if you have logged on from a secondary terminal, or if there is only one customer.

2 Press the [Delete] softkey.

Result: You are prompted for the customer number.

Step	Action
3	Enter the number of the customer you want to delete and press Return. **Result:** The Delete Customer screen is displayed.

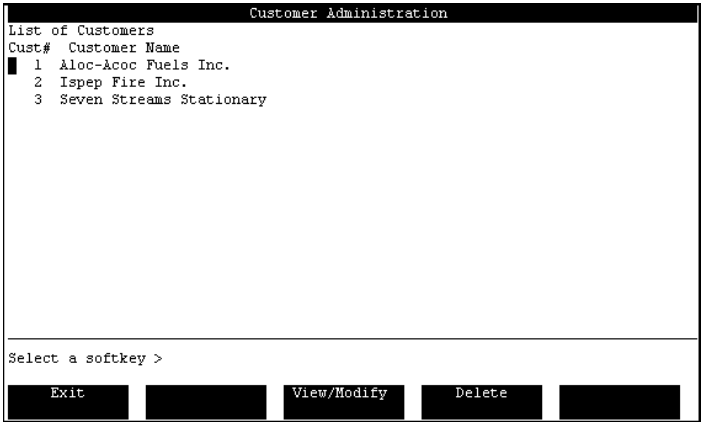
4	Is this the customer you want to delete? • If yes, press the [OK to Delete] softkey. **Result:** The customer is deleted and you are prompted for another customer number. • If no, press the [Cancel] softkey.

Deleting a customer when you do not know the customer number

If you do not know the customer number of the customer you want to view or modify, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Follow the procedure for finding customers on page 5-14 and then return to this procedure. **Note:** Use the [List] softkey to get a list of customers.



Note: The [Delete] softkey is not displayed if you have logged on from a secondary terminal, or if there is only one customer.

2 Select the customer you want to delete by putting the cursor on that customer and pressing the space bar.

3 Press the [Delete] softkey.

Result: The Delete Customer screen is displayed.

Step	Action
4	Is this the customer you want to delete? • If yes, press the [OK to Delete] softkey. **Result:** The customer is deleted and you are prompted for another customer number. • If no, press the [Cancel] softkey.

Chapter 6

Making voice recordings

In this chapter

Overview	6-2
Types of recordings	6-4
How Call Answering uses personal greetings and personal verifications	6-7
Voice recording tips	6-11
Section A: Making recordings	6-13
Section B: VMUIF recordings	6-47

Overview

Introduction

As administrator, you make two types of voice recordings: those used only for administrative purposes, and those played to the public or other users. You make these recordings through the administration terminal (with a telephone nearby) or by using a telephone handset alone.

This chapter provides information and procedures for making different kinds of voice recordings or, where necessary, refers you to other chapters or manuals for this information.

The overview presents an introduction to the types of voice recordings you can make. It also offers some guidelines for making voice recordings.

Administration level

You can make voice recordings from either the System Administration level or the Customer Administration level.

However, at the System Administration level, you can only view, modify, or delete recordings. You cannot add new recordings from that level.

The voice recordings that you can add at the Customer Administration level only include

- announcement definitions
- Thru-Dial definitions
- voice menu definitions

Section A

Section A presents information and procedures for logging in to Meridian Mail and creating, playing back, editing, and deleting recordings.

These recordings include the following:

- the call answering greeting
- personal verifications (which can be recorded by you or the users on your system)
- system distribution list personal verifications
- remote site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings (announcements, Thru-Dial services, Fax on Demand, voice menus, and Voice Prompt Maintenance)

For your reference, Section A also presents an overview of some of the voice recordings that users on your system make. These include the following:

- personal greetings
- broadcast messages

For more information about the recordings users can make, refer to the *Meridian Mail Voice Messaging User Guide* (P0875935).

Section B

Section B provides information and procedures for the greetings and introductory tutorials available for the VMUIF interface.

For information about making recordings for Hospitality systems, refer to the *Hospitality Voice Services Implementation Guide* (NTP 555-7001-221) and to the *Hospitality Voice Services Guest Administration Console Guide* (NTP 555-7001-222).

Types of recordings

Introduction

You can make different kinds of voice recordings from the administration terminal and a telephone or from a telephone handset alone. This overview presents an introduction to these recordings.

Call answering greeting

When MMUI is installed on your system, the call answering greeting identifies your organization to external callers. This greeting is not available if VMUIF is installed.

You record the call answering greeting from the administration terminal or from a telephone handset with administrator capabilities.

For information and procedures, see “Recording a call answering greeting” on page 6-18.

Personal greetings

If MMUI is installed on your system, users can record three kinds of personal greetings from their telephone handsets: external, internal, and temporary greetings.

If VMUIF is installed, users can record external and internal greetings.

For information and procedures, see “Recording personal greetings” on page 6-24. You may also wish to refer to the *Meridian Mail Voice Messaging User Guide* (P0875935). For information on how Meridian Mail decides which prompts, personal greetings, and personal verifications to play during an individual Call Answering session, see “How Call Answering uses personal greetings and personal verifications” on page 6-7.

Personal verification

The personal verification is used to identify local, remote, or directory entry users. Typically, it is recorded by the users themselves from their telephones, but you can also record it from the administration terminal as you add a user to the system or if you are logged into a mailbox as administrator.

For information and procedures, see “Recording a personal verification” on page 6-26. For information on how Meridian

Mail decides which prompts, personal greetings, and personal verifications to play during an individual Call Answering session, see "How Call Answering uses personal greetings and personal verifications" on page 6-7.

System distribution list personal verification

The system distribution list personal verification is an optional recording. This verification helps you to confirm you have selected the correct distribution list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

For information and procedures, see "How Call Answering uses personal greetings and personal verifications" on page 6-7.

Remote site name verification

The site name verification is available if MMUI is installed on your system. It works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For information and procedures, see "Identifying remote site names" on page 6-34, and refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Broadcast mailbox personal verification

Broadcast mailboxes can be set up for both the MMUI and VMUIF interface.

A broadcast message is a message that is sent to all Meridian Mail users.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *"Broadcast mailbox 5555."*

For information and procedures, see "Recording a personal verification for the broadcast mailbox" on page 6-38.

Broadcast messages

A broadcast message is a message that is sent to all Meridian Mail users.

When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all of the users on the system. If you have Meridian Mail Networking, you can choose to send broadcast messages to all users at a particular Networking remote site, or at a group of sites.

For more information and procedures, see "Recording and sending broadcast messages" on page 6-41.

Voice Services recordings

The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recordings, Thru-Dial greetings, fax item confirmation prompts, voice menu greetings, voice menu choices, and voice menu prompts.

For more information and procedures, see "Making Voice Services recordings" on page 6-44, and refer to the *Voice Services Application Guide* (NTP 555-7001-325).

How Call Answering uses personal greetings and personal verifications

Introduction

Call Answering is the collection of Meridian Mail features which deals with directing callers to a user's mailbox when

- the user does not answer his or her phone
- the call has been transferred directly to the mailbox by a Call Answering DN
- the DN is busy with another call

There is a variety of prompts Meridian Mail can play to a caller, depending on which prompts have been recorded, where the call originates, and the mailbox user's Class of Service settings. The charts below show how Meridian Mail decides which prompts to play during an MMUI Call Answering session.

VMUIF users

Call Answering is simpler for VMUIF mailbox users.

Call Answering - no answer/call transferred to mailbox

1. Is there a greeting recorded?

   If yes, play the greeting.

   If no, play the standard system "Nobody is available to take your call..." message.

Call Answering - user busy

1. Play the standard system "This line is busy..." message.
2. Is there a greeting recorded?

   If yes, play the greeting.

   If no, proceed to the next step.

3. Play the standard system "Please leave a message after the tone..." message.

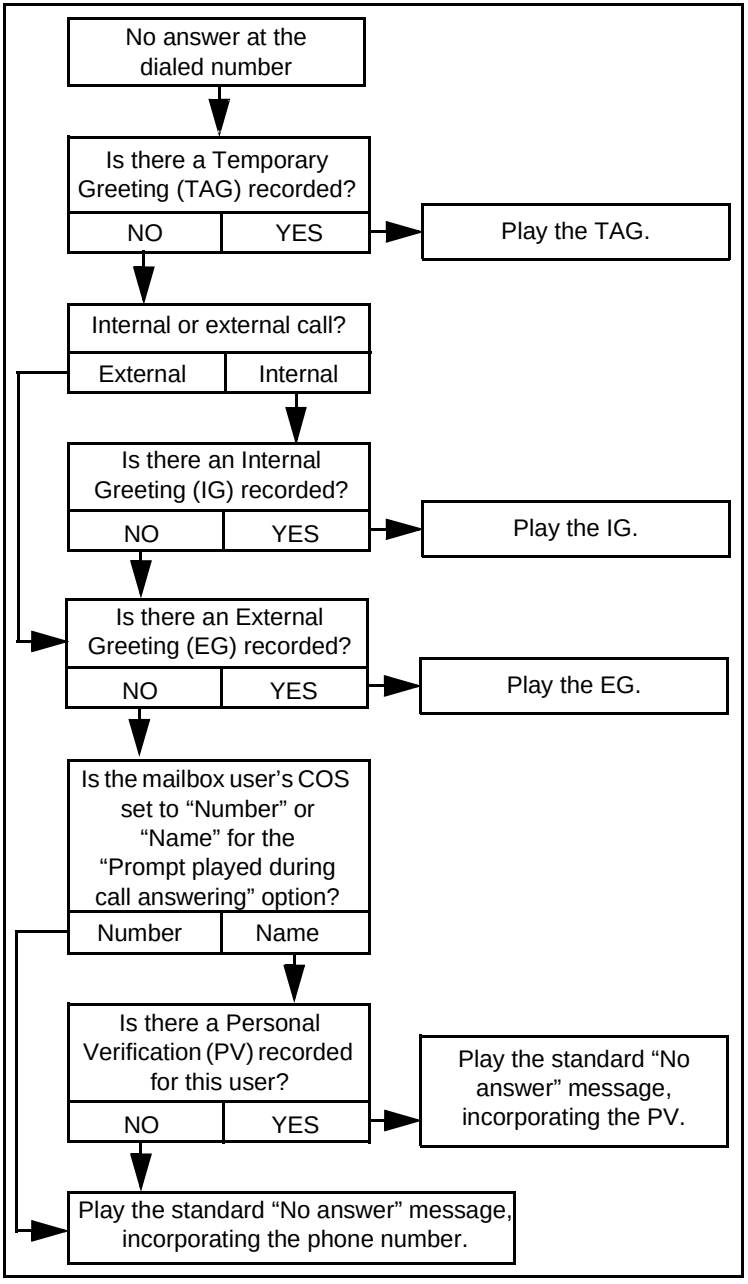
HVS Staff and Guest users

HVS Staff users are treated as MMUI mailbox users.

HVS Guest users behave as VMUIF mailbox users.

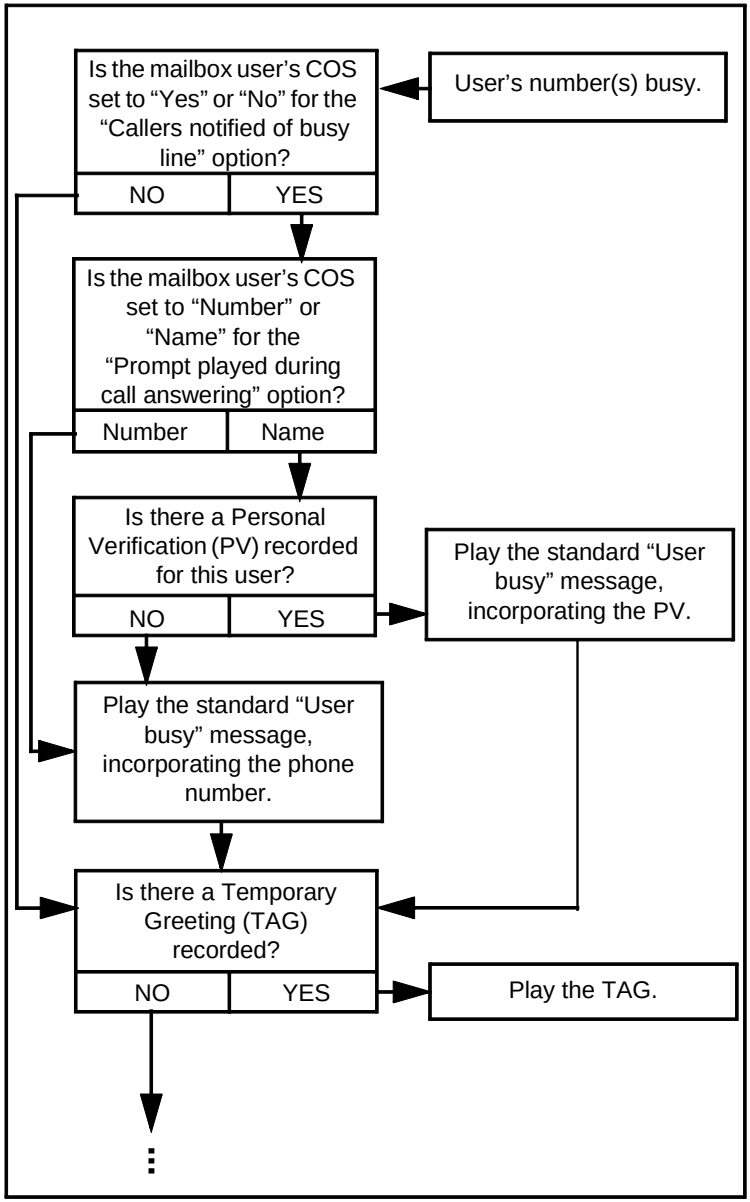
Call Answering - no answer/call transferred to mailbox

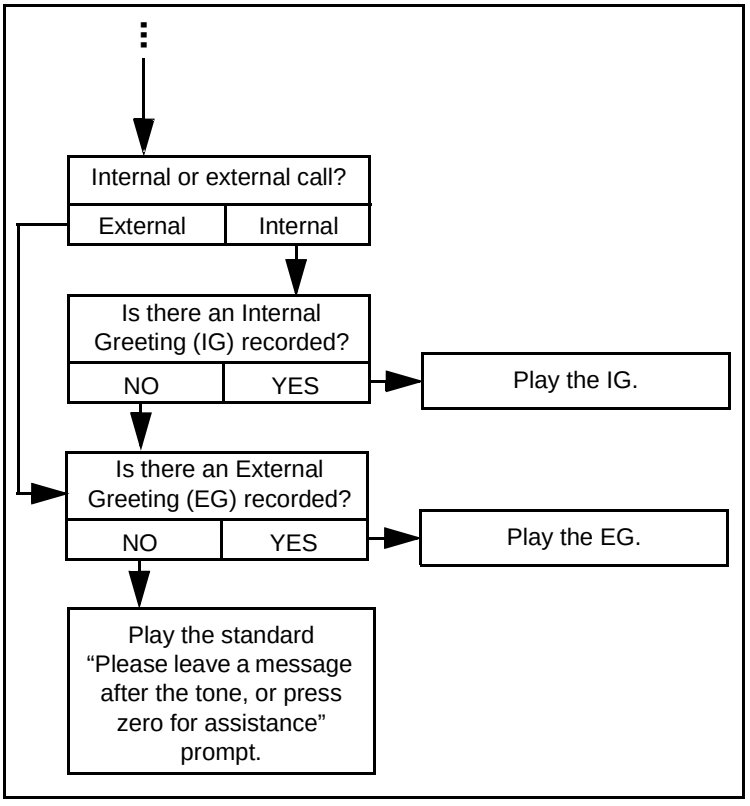
This is how Meridian Mail decides which prompt(s) to play to a caller when a mailbox user does not answer his or her phone, or when a Call Answering DN has sent the call directly to the mailbox.


No answer at the dialed number
Is there a Temporary Greeting (TAG) recorded?
NO
YES
Play the TAG.
Internal or external call?
External
Internal
Is there an Internal Greeting (IG) recorded?
NO
YES
Play the IG.
Is there an External Greeting (EG) recorded?
NO
YES
Play the EG.
Is the mailbox user's COS set to "Number" or "Name" for the "Prompt played during call answering" option?
Number
Name
Is there a Personal Verification (PV) recorded for this user?
NO
YES
Play the standard "No answer" message, incorporating the PV.
Play the standard "No answer" message, incorporating the phone number.

Call Answering - user busy

This is how Meridian Mail decides which prompt(s) to play to a caller when a mailbox user's phone is already busy.


Is the mailbox user's COS set to "Yes" or "No" for the "Callers notified of busy line" option?
User's number(s) busy.
NO
YES
Is the mailbox user's COS set to "Number" or "Name" for the "Prompt played during call answering" option?
Number
Name
Is there a Personal Verification (PV) recorded for this user?
NO
YES
Play the standard "User busy" message, incorporating the PV.
Play the standard "User busy" message, incorporating the phone number.
Is there a Temporary Greeting (TAG) recorded?
NO
YES
Play the TAG.


Internal or external call?
External
Internal
Is there an Internal Greeting (IG) recorded?
NO
YES
Play the IG.
Is there an External Greeting (EG) recorded?
NO
YES
Play the EG.
Play the standard "Please leave a message after the tone, or press zero for assistance" prompt.

Voice recording tips

Introduction

As administrator, you make two types of voice recordings:

- prompts that are used only for administrative purposes (such as broadcast mailbox personal verifications or system distribution list personal verifications)
- recordings played to the public or other users (such as the call answering greeting, personal verifications, remote site name verifications, and Voice Services recordings such as announcements, Thru-Dial services, Fax on Demand, or voice menus)

Prompts used only for administrative purposes require little preparation after you decide on their wording.

Voice menus or announcements played to the public or other users may require more formal preparation. For more information, you may wish to refer to the *Voice Services Application Guide* (NTP 555-7001-325).

Guidelines for voice recordings

The following are some suggestions for making voice recordings:

- Use only one voice for your voice recordings, so that callers are not distracted by changes in pitch, tone, intonation, or accent.
- To select a person to make your voice recordings, begin by auditioning a few candidates. Record their voices and then listen to the recordings over the telephone line. Low-pitched voices reproduce better than high-pitched voices over telephone lines. The voice used for the Meridian Mail prompts provides a good model.
- Print out complete, definitive copies of the script.
- Record in quiet surroundings.

  Start recording immediately after the tone, and stop the recording immediately after the last word. This prevents unnecessary pauses when system prompts and personal verifications are joined.

Guidelines for voice recordings (cont'd)

- To stop recording, press the number sign (#) if you are recording from a telephone handset, or the [Stop] softkey if you are recording from the administration terminal. Do not hang up the phone while you are recording as this may produce clicks in the recording.
- For applications that provide current information, have the person who knows the information monitor the prompts to ensure that the information is always up-to-date.

Section A: Making recordings

In this section

Overview	6-14
Logging in to Meridian Mail	6-15
Recording a call answering greeting	6-18
Recording personal greetings	6-24
Recording a personal verification	6-26
Recording a personal verification for a system distribution list	6-31
Identifying remote site names	6-34
Recording a personal verification for the broadcast mailbox	6-38
Recording and sending broadcast messages	6-41
Making Voice Services recordings	6-44

Overview

Introduction

This section presents information and procedures for logging in to Meridian Mail from the administration terminal or from a telephone on your system. It also explains how to create, play back, edit, and delete voice recordings.

Logging in to Meridian Mail

Introduction

Before you can create, play back, modify, or delete voice recordings, you need to log in to Meridian Mail. You do this either through a telephone set or through an administration terminal with a telephone nearby.

About using the telephone to make recordings

Using a telephone on your system, you or the users on your system log into Meridian Mail and access personal greetings. You can then make a number of kinds of voice recordings:

- external, internal, and temporary absence greetings
- personal verifications
- broadcast messages

About using a terminal to make recordings

Using the administration terminal or a telephone set with administrator capabilities, you can make certain kinds of recordings:

- the call answering greeting
- personal verifications
- system distribution list personal verifications
- site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings

To make recordings through the system interface, the [Voice] softkey must be displayed.

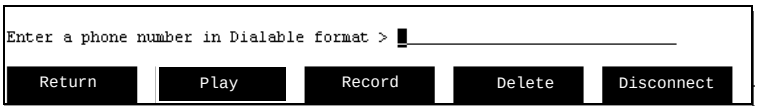
Note: A telephone set is required to make recordings through the administration terminal. Ensure that a phone set is available near the administration terminal where you are working.

Screens with recording softkeys

Recording softkeys are available from some of the User Administration screens and Voice Services Administration screens.

Recording softkey positions

The following shows typical recording softkey positions.



Logging in using a telephone

To log in to Meridian Mail using a telephone set, follow these steps.

Step	Action
1	Dial the Meridian Mail access number.
2	Use the following table to determine the next step.

IF you are logging in from	THEN
your own telephone	press #.
another touch tone telephone	using the telephone keypad, enter your mailbox number, and press #.

Step	Action
3	Enter your password using the telephone keypad, and press #.
4	Use the following table to determine the next step.

IF you want to	THEN
create, play back, modify, or delete an internal greeting	see “Recording personal greetings” on page 6-24.
create, play back, modify, or delete an external greeting	see “Recording personal greetings” on page 6-24.
create, play back, modify, or delete a temporary absence greeting	see “Recording personal greetings” on page 6-24.
create, play back, or delete a personal verification	see “Recording a personal verification” on page 6-26.

Logging in from the administration terminal

To log in to Meridian Mail from the administration terminal, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select [Logon]. **Result:** The system prompts you for a password.
2	Use the following table to determine the next step.

IF	THEN
you are logging in the first time	"Setting the customer administration password" on page 3-8.
you have logged in before	go to step 3.

Step	Action
3	Type your customer administration password, and press <Return>. **Result:** The system displays the Customer Administration Menu. **Note:** If an invalid password is entered, an error message appears. Return to step 1.
4	Use the following table to determine the next step.

IF you want to record	THEN
the call answering greeting	see "Recording personal greetings" on page 6-24.
a personal verification	see "Recording a personal verification" on page 6-26.
a personal verification for a system distribution list	see "How Call Answering uses personal greetings and personal verifications" on page 6-7.
a personal verification for a remote site name	see "Identifying remote site names" on page 6-34.
a broadcast mailbox personal verification	see "Recording a personal verification for the broadcast mailbox" on page 6-38.
make Voice Services recordings	see "Making Voice Services recordings" on page 6-44.

Recording a call answering greeting

Introduction

This topic provides information and procedures for recording a call answering greeting.

When you have MMUI installed, the call answering greeting identifies your organization to callers and users. Typically, this greeting consists of the spoken name of the organization.

The call answering greeting is played when

- an external caller is transferred to Meridian Mail to leave a message
- a user answers a remote notification call

Note: This greeting is available only if the MMUI interface is installed on your system. It is not available if VMUIF is installed.

You record the call answering greeting from the administration terminal or from a telephone set with administrator capability.

Using the call answering greeting

This greeting is optional. If you record the greeting, external callers hear it before they hear a user's personal greeting. If no greeting is recorded, callers hear only the user's personal greeting when they connect to a mailbox.

During remote notification calls, the following prompt is played to users if no call answering greeting is recorded: *"Hello. Meridian Mail has received a message for ...."*

When a call answering greeting exists, the following prompt is played: *"Hello. <Call Answering Greeting> has received a message for ...."*

Guidelines for composing

The following are some guidelines for composing a call answering greeting:

- Because this greeting is used in a variety of situations, consider how best to word it (or decide whether you want to record a greeting at all).
- If you do not record a call answering greeting, your organization's name is not announced at the beginning of a call answering session. If you feel that the user's personal greeting is sufficient, you may regard the call answering greeting as unnecessary.
- If you record only the organization's name ("*Myelin Incorporated"*), the greeting played during call answering may be too abrupt, but the prompt played during remote notification sounds quite natural.
- A friendlier greeting ("*Thank you for calling Myelin Incorporated"*) is ideal for call answering but is awkward when it is played for remote notification.

Multilingual systems

If more than one language is installed on your Meridian Mail system and you want to record a call answering greeting, you need to record one greeting for each language.

Recording the call answering greeting from a telephone set

To record, play back, modify, or delete the call answering greeting from a telephone set with administrator capabilities, follow these steps.

Step	Action
1	Press **82** on the telephone keypad.
2	Press **9** for the system greeting.
3	Use the following table to determine the next step.

IF you want to	THEN
review the greeting	go to step 4.
delete the greeting	go to step 5.
rerecord the greeting	go to step 5.
add to the greeting	go to step 6.

Step	Action
4	To review the greeting, press **2**.
5	To delete the greeting, press **76**. **Note:** If you do not delete the existing greeting, your new recording is appended to it.
6	To begin recording or add to the greeting, press **5**.
7	At the tone, record the call answering greeting.
8	To stop recording, press #. **Note:** Do not hang up the phone during recording as this may produce a click sound.
9	To review the greeting, press **2**.
10	To end your voice messaging session, press **83**, and then hang up.

Administration level

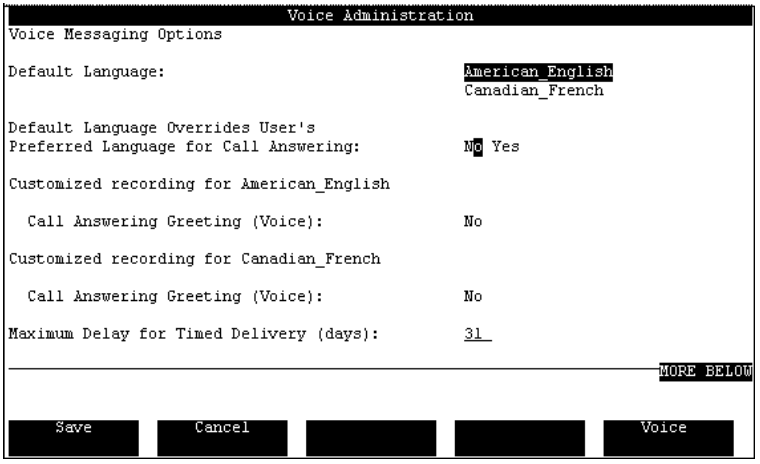
You can create, play back, modify, or delete a call answering greeting through the administration terminal from the Customer Administration level only.

Procedure

To create, play back, modify, or delete a call answering greeting through the administration terminal, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.



3	Move the cursor to the first Call Answering Greeting (Voice) field.
4	Select the [Voice] softkey. **Result:** The current screen remains displayed; the softkey display changes to [Cancel]. The system prompts for an extension number.
5	Type the extension number of the telephone set you will use to make the recording, and press <Return>. **Result:** The phone rings.
6	Pick up the telephone handset. **Result:** The system displays the recording softkeys.

Step	Action
7	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
8	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the greeting exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
9	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
10	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 13.
record the greeting again	go to step 7.
save the recording	go to step 17.

Step	Action
11	Select the [Play] softkey. **Result:** If a recording is available, it is played. The system displays the [Stop] softkey. **Note:** If there is no current recording, the system displays a message on the console.
12	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
13	To delete the recording, select the [Delete] softkey. **Result:** The system displays the [OK to Delete] and [Cancel] softkeys. You are requested to confirm the deletion.
14	Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 15.
confirm the deletion	go to step 16.

Step	Action
15	To cancel the deletion, select the [Cancel] softkey. **Result:** The recording is not deleted. The system again displays the recording softkeys.
16	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
17	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
18	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording personal greetings

Introduction

You and the users on your system record personal greetings—external, internal, and temporary greetings—from the telephone. These recordings are played when callers connect to a mailbox. The external greeting is played to external callers, the internal greeting is played to internal callers, and the temporary greeting, when one is recorded, preempts both internal and external greetings. The temporary greeting is commonly used for short-term messages to notify all callers that the mailbox user is away sick that day, or on vacation, or to otherwise alter the user's greeting on the short term.

This is an overview of personal greetings. For more information, refer to the *Meridian Mail Voice Messaging User Guide* (P0875935). For information on which personal greetings are used during a Call Answering session, see "How Call Answering uses personal greetings and personal verifications" on page 6-7.

Note: If VMUIF is installed on your system, users can record only external and internal greetings.

Recording personal greetings

To create, play back, modify, or delete a personal greeting, follow these steps.

Note: You must be logged in to a Meridian Mail mailbox. See "Logging in to Meridian Mail" on page 6-15.

Step	Action
1	Press **82** on the telephone keypad.
2	Select an external, internal, or temporary personal greeting.

IF you want to select	THEN
your external greeting	press **1**.
your internal greeting	press **2**.
your temporary greeting	press **3**.

Result: The system confirms the greeting you select.

3 Use the following table to determine the next step.

IF you want to	THEN
review your greeting	go to step 4.
delete your greeting	go to step 5.
record your greeting again	go to step 5.
add to your greeting	go to step 6.
set an expiry date for your temporary greeting	go to step 9.

4 To review the greeting, press **2**.

5 To delete the greeting, press **76**.

Note: If you do not delete your existing greeting, your new recording is appended to it.

6 To begin recording or add to the greeting, press **5**.

7 At the tone, record your greeting.

8 To stop recording, press #.

Note: Do not hang up the phone during recording as this may produce a click sound.

9 To set the expiry date for your temporary greeting, press **9**.

Note: Whenever you log in to your mailbox, the system prompts that you are using a temporary greeting.

10 To end your voice messaging session, press **83**, and then hang up.

Recording a personal verification

Introduction

This topic provides information and procedures for recording a personal verification using either a telephone handset alone or the administration terminal and a telephone.

The personal verification is a recording of a user's first and last names (and extension, if desired). It is used to identify the owner of a mailbox. Ideally, users should record personal verifications in their own voice. However, as administrator, you can record personal verifications for users either from the administration terminal or from a telephone set with administrator capabilities.

Using a personal verification

A personal verification is played in the following situations:

- Call Answering can be activated by a caller encountering a busy/unanswered DN, or by a caller calling a Call Answering service DN which directs the call to a particular mailbox.

  In Call Answering, the personal verification is played when the called number is busy. It is also played when the called number does not answer, and no personal greeting has been recorded. See "How Call Answering uses personal greetings and personal verifications" on page 6-7. for a complete explanation of the use of personal verifications in Call Answering.
- During message composition, the system plays the verification after a user enters a mailbox number to verify that the correct person is being addressed.
- When a user receives a message, the system plays the verification to identify who the message is from (such as the system administrator) or to advise all recipients that the message is a broadcast message.
- When messages are delivered to nonusers (using the Delivery to Non-Users feature), the system includes the verification. Recipients are more likely to listen to messages if they recognize who the messages are from.

- When callers use the Name Dialing feature, the system plays the personal verification. If a personal verification has not been recorded, the system spells out the name instead.
- During remote notification, the system plays the verification to identify who the message is intended for.

No personal verification recorded

If no verification is recorded, the system plays a recording of the user's extension number. Because it is easier for callers to confirm they have reached the correct person by hearing a name rather than by hearing an extension number, it is highly recommended that you or the users on your system record a personal verification for each mailbox.

Who can change personal verifications

Users can change their personal verifications only if this capability is enabled in the class of service to which they are assigned. For more information, see Chapter 27, "Class of Service administration".

Guidelines for composing

The following are some suggestions for recording personal verifications:

- Record a few names for personal verification, and listen to them before recording the remaining names.

  This ensures that the procedure is done correctly and the intonation is good. Test each of the following areas where personal verification applies:

  - call answering
  - message envelope playback
  - address playback in the compose command
  - name dialing
  - name addressing
  - express messaging
  - delivery to non-user
- When you are recording a personal verification for two or more people in your organization who have the same name (or very similar names), provide more information (their extension number or title, for example) to distinguish them.

Recording a personal verification using a telephone

To create, play back, or delete a personal verification using a telephone handset, follow these steps.

Note: You must be logged in to a Meridian Mail mailbox. See "Logging in to Meridian Mail" on page 6-15.

Step	Action
1	Press **89** on the telephone keypad. **Result:** The system plays the existing name for personal verification. If no name is recorded, the system reports this.
2	Use the following table to determine the next step.

IF you want to	THEN
hear the name for personal verification again	go to step 3.
record a new personal verification	go to step 4.
delete the existing personal verification	go to step 8.

3	To hear the name for personal verification again, press **2**.
4	To record a new personal verification, press **5**.
5	At the tone, record your greeting. **Note:** The maximum length is 20 seconds.
6	To stop recording, press #. **Result:** The system replays your recording.
7	To add to the recording, press **5**, and repeat step 5 and step 6.
8	To delete the existing personal verification, press **76**.
9	To end your voice messaging session, press **83**, and then hang up.

Administration level

You can create, play back, or delete a personal verification from the administration terminal from the Customer Administration level only.

Recording a personal verification through the administration terminal

To create, play back, or delete a personal verification from the administration terminal, follow these steps.

Starting Point: The Customer Administration Menu

1 Select User Administration.

2 Select Local Voice User.

3 Select the [View/Modify] softkey, and type the mailbox number of the user whose personal verification you want to record.

Result: The system displays the View/Modify Local Voice User screen.

4 Select the [Voice] softkey.

Result: The current screen remains displayed; the softkey display changes to [Cancel].

The system prompts for an extension number.

5 Type the extension number of the telephone set you will use to make the recording, and press <Return>.

Result: The phone rings.

6 Pick up the telephone handset.

Result: The system displays the recording softkeys.

7 Select the [Record] softkey.

Result: The system displays the [Stop] softkey in place of the [Record] softkey.

You hear a tone through the telephone receiver.

8 At the tone, begin speaking into the receiver.

Note: Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.

9 To stop recording, select the [Stop] softkey.

Result: The recording stops automatically, and the system again displays the recording softkeys.

10 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.

11 To review your recording, select the [Play] softkey.

Result: The system plays the recording.

The system displays the [Stop] softkey.

12 To stop the playback at any time, select the [Stop] softkey.

Result: The system again displays the recording softkeys.

13 To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.

Result: The system displays the original softkeys.

Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.

When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.

14 To delete a personal verification, use the arrow keys to select the entry, select the name using the spacebar, and press [Delete].

Result: The system displays the [OK to Delete] and [Cancel] softkeys.

15 Select [OK to Delete] to delete the personal verification.

Result: The system deletes the personal verification and updates the list.

16 To update the screen and store the changes to the recording, use the [Save] softkey.

Recording a personal verification for a system distribution list

Introduction

It is a good idea to make a voice recording of the title of each system distribution list. This procedure is optional, but a voice title helps you to confirm you have selected the correct list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

Administration level

You can record a personal verification for a customer distribution list from the Customer Administration level only.

Procedure

To record a personal verification for a system distribution list, follow this procedure.

Note: This procedure is optional.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Distribution Lists. **Result:** The system displays the Distribution Lists softkeys screen.
3	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
4	Type the number of the distribution list for which you are recording a title.
5	Select the [Voice] softkey. **Result:** The system prompts for an extension number.
6	Type the extension number of the telephone set you are going to use to record the title, and press <Return>. **Result:** The phone rings.
7	Pick up the telephone handset. **Result:** The system displays the recording softkeys.

Step	Action
8	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
9	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile. At the tone, record the personal verification.
10	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
11	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 8.

Step	Action
12	To review your recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
13	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
14	To delete the recording, select the [Delete] softkey. **Result:** The system displays the [OK to Delete] and [Cancel] softkeys. You are requested to confirm the deletion.
15	Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 16.
confirm the deletion	go to step 17.

Step	Action
16	To cancel the deletion, select the [Cancel] softkey. **Result:** The recording is not deleted. The system again displays the recording softkeys.

Step	Action
17	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
18	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
19	To update the screen and store the changes to the recording, use the [Save] softkey.

Identifying remote site names

Introduction

The site name verification works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site. A site name can be recorded for Meridian Mail network sites.

If no site name is recorded, the system instead plays a recording of the site number that identifies the site.

For more information, refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Remote site name verification

The site name verification is available if MMUI is installed on your system. It works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For more information, refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Administration level

You can record a site name verification from the Customer Administration level only.

Procedure

To record a site name verification, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select Network Administration.
2	Select the type of networking administration.
3	Select the type of site maintenance.
4	Select the [Add] softkey for a new site or the [View/Modify] softkey for an existing site.
5	Select the [Voice] softkey. **Result:** The current screen remains displayed; the softkey display changes to [Cancel]. The system prompts for an extension number.
6	Type the extension number of the telephone set you will use to make the recording, and press <Return>. **Result:** The phone rings.
7	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
8	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
9	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
10	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.

Step	Action

11 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.
save the recording	go to step 18.

12 To review your recording, select the [Play] softkey.

Result: The system plays the recording.

The system displays the [Stop] softkey.

13 To stop the playback at any time, select the [Stop] softkey.

Result: The system again displays the recording softkeys.

14 To delete the recording, select the [Delete] softkey.

Result: The system displays the [OK to Delete] and [Cancel] softkeys.

You are requested to confirm the deletion.

15 Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 15.
confirm the deletion	go to step 16.

16 To cancel the deletion, select the [Cancel] softkey.

Result: The recording is not deleted.

The system again displays the recording softkeys.

Step	Action
17	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
18	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
19	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording a personal verification for the broadcast mailbox

Introduction

This topic provides information and procedures for recording a personal verification for the broadcast mailbox.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *"Broadcast mailbox 5555."*

To set up a broadcast message, a special mailbox number (the broadcast mailbox number) is defined in the Voice Messaging Options screen. When you compose a broadcast message, you specify this broadcast mailbox number, and all users receive your message.

Administration level

You can record a personal verification for the broadcast mailbox from the Customer Administration level only.

Recording from the administration terminal

To record a personal verification for the broadcast mailbox from the administration terminal, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options.
3	Move the cursor to the Broadcast Mailbox Personal Verification Recorded (Voice) field.
4	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
5	Type the extension of the phone you will use to record the verification, and press <Return>. **Result:** The phone rings.

Step	Action
6	Pick up the receiver. **Result:** The recording softkeys are displayed.
7	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
8	At the tone, say the verification. **Example:** *"Broadcast mailbox 5555."*
9	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
10	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
save the recording	go to step 13.
rerecord the recording	press the [Delete] key, and go to step 7.

11	To play back the recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.

Step	Action
12	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
13	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
14	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording and sending broadcast messages

Introduction

This topic explains how you and the users on your system can record and send broadcast messages using the telephone handset.

Definition: broadcast message

A broadcast message is a message that is sent to all Meridian Mail users. When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all users on your Meridian Mail system.

Administration level

You cannot send a broadcast message to all users on a multi-customer system. You can only reach all the users of the customer which owns the mailbox you are using to send the message.

For example, you may set each customer's broadcast mailbox number to 999, but when you log on to a mailbox that belongs to Customer X, only this customer's users will receive the message.

Network broadcast message option for Meridian Mail Networking users

Customers who have Meridian Mail Networking (either Meridian Networking or Enterprise Networking) can choose to send broadcast messages to all users at

- a single site, either the local one or a remote one
- a combination of sites (this involves putting in the network prefix numbers and broadcast mailbox number for each site, or incorporating them into a Personal Distribution List)
- all sites

Network broadcast messages sent to multi-customer remote systems will only be delivered to users in the networking customer group.

Enabling network broadcast messaging

To enable network broadcast messaging, you must fill in the Network Broadcast Administration fields when configuring

Networking in the Network Configuration screen. See your Network Administration books for details.

You must also record a personal verification for the local broadcast mailbox (see "Recording a personal verification for the broadcast mailbox" on page 6-38.) Otherwise, network broadcast messaging will not work.

Restrictions on network broadcast messages

A user must have "Broadcast Capability" and "Network Broadcast Capability" set to "Yes" in their Class of Service to send network broadcast messages.

The acknowledgment message tag cannot be applied to network broadcast messages, or to any Personal Distribution List containing a network broadcast address, because this could result in the system attempting to return thousands of messages to the sender.

Network broadcast messages can only be sent to sites running MM11 and later releases. Network broadcast messages sent to MM10 and earlier releases will fail, with no NDN delivered to the sender.

Setting up a broadcast mailbox

To set up a broadcast mailbox, you assign a mailbox number to the broadcast mailbox in the Voice Messaging Options screen. You do not need to set up an actual mailbox through User Administration. For more information about setting up broadcast mailboxes, see Chapter 21, "Voice messaging options".

Who can compose and send broadcast messages

Any user who knows the broadcast mailbox number and has access to a mailbox with broadcast capability can compose and send broadcast messages. It is recommended that users try to avoid sending broadcast messages during busy hours.

Administration level

You can only record a broadcast message for the users of one customer at a time. To send the message to multiple customers' users, you must repeat the login and recording process for each customer.

Procedure To record and send a broadcast message, follow these steps.

Step	Action
1	Log on to a Meridian Mail mailbox that belongs to the customer to which you want to send the broadcast message. **Note:** The mailbox must have broadcast capability.
2	Press **75**, and enter a number to specify the type of broadcast message you want.

IF you want to send a broadcast message to all users at	THEN enter
this site	nothing.
a particular remote Meridian Mail Networking site	the site's Network Prefix. (If your system uses overlap in its Network Prefixes, ignore the overlap and use the entire prefix.)
all sites, local and remote	the Network-Wide Broadcast Prefix. (This is set through the Network Configuration screen. See your Network Administration guide.)

3	Enter the broadcast mailbox number for your local Meridian Mail system (the default is 5555), and press #.
4	Repeat step 2 and step 3 to add other broadcast destinations to the list, if desired.
5	Press # again, to end the list.
6	To start recording, press **5.**
7	At the tone, record your broadcast message.
8	To stop recording, press **#**.
9	To listen to your broadcast message, press **2**.
10	To send the broadcast message, press **79**.
11	To end your voice messaging session, press **83**, and then hang up.

Making Voice Services recordings

Introduction

The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recording, Thru-Dial greetings, fax item confirmation prompts, voice menu greetings, voice menu choices, and voice menu prompts.

This topic provides an overview of making Voice Services recordings. For more information and more detailed procedures, refer to the *Voice Services Application Guide* (NTP 555-7001-325).

Announcements

This service enables you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly by a caller.

Thru-Dial services

These services access predefined DNs or user-prompted DNs that can be used within a voice menu service or as a separate service with a directory number. Thru-Dial services can be created to provide a variety of dialing options to users of Meridian Mail.

Fax on Demand

Fax on Demand is a Meridian Mail feature that allows a caller to obtain information in the form of a fax. Depending on the configuration of this feature on a system, fax documents may be stored either as stand-alone, directly dialed fax items, or as items selected from voice menus.

Voice Menus

The Voice Menus service enables you to create single-layered or multilayered menus that present choices to callers. Callers make their selections by pressing the key on the telephone keypad that corresponds to the action they wish to perform.

Voice Prompt Maintenance

This service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

Administration level

You can make a voice services recording from either the System Administration level or the Customer Administration level.

Procedure

To make a Voice Services recording, follow these steps.

Starting Point: The Main Menu or The Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Select the type of voice service.
4	Use the following table to determine the next step.

IF you want to	THEN
create a new Voice Service recording	select the [Add] softkey.
add a new voice recording to an existing voice service	select the [View/Modify] softkey.
modify an existing voice recording	select the [View/Modify] softkey.

5 Use the following table to determine the next step.

IF you want to make	THEN move the cursor to the
an Announcement recording	Announcement Recorded field.
a Thru-Dial recording	Greeting Recorded field.
a Fax Item recording	Continuation Prompt Recorded field.
a Voice Menu recording	Greeting Recorded field or Menu Choices Recorded field.
a Voice Form recording	Form Name Recorded field.

6 Select the [Voice] softkey.

7 Type the extension of the phone you will use to make the recording, and press <Return>.

Result: The phone rings.

Step	Action
8	Pick up the receiver. **Result:** The recording softkeys are displayed.
9	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
10	At the tone, make your recording.
11	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
12	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 13.
save the recording	go to step 15.
rerecord the recording	press the [Delete] key, and go to step 9.

13	To play back the recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
14	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.

Section B: VMUIF recordings

In this section

Overview 6-48
VMUIF introductory tutorials and the VMUIF login greeting 6-49
Recording the VMUIF login greeting 6-52

Overview

Introduction

Three recordings are prerecorded for the VMUIF interface:

- the introductory tutorial (for touch tone users)
- the introductory tutorial (for dial pulse users)
- the login greeting

These default recordings are enabled by default.

You can use these default recordings, customize them, or disable them.

This section provides information and procedures for the tutorials and greeting.

VMUIF introductory tutorials and the VMUIF login greeting

Introduction

An introductory tutorial greeting is played to VMUIF subscribers the first time they log in to their mailboxes. This tutorial familiarizes them with the Meridian Mail system.

The default DTMF tutorial

The Meridian Mail system plays the following introductory tutorial the first time a user logs in to a new mailbox from a touch tone telephone (a dual tone multifrequency or DTMF phone).

"You are about to hear an introduction to Call Answering. This service will allow your callers to leave you recorded messages. You can play back your messages from your home phone, or, if you create a password, from any touch tone phone outside your home. You can also record a personalized greeting that will be played to your callers, and you can erase your messages right away, or store them temporarily in your mailbox. Step-by-step instructions will guide you through your sessions. And remember, for help at any time, just press zero."

The default dial pulse tutorial

The Meridian Mail system plays the following introductory tutorial the first time a user logs in to a new mailbox that is set up as a dial pulse user.

"You are about to hear an introduction to Call Answering. This service will allow your callers to leave you recorded messages. You can listen to your messages from your home phone at any time. You can also play your messages from any touch tone phone. And by calling the Greeting Change Service, you can record a personalized greeting that will be played to your callers. Step-by-step instructions will guide you through your sessions. Consult the brochure for more information."

The login greeting

The login greeting is played when subscribers log on to Meridian Mail.

"Welcome to Call Answering."

The custom tutorial

You may prefer to record a custom tutorial to address particular needs of users on your system.

In preparing your tutorial, you may wish to refer to the text of the default tutorials in this section.

Administration level

You can record or disable the VMUIF tutorial from the Customer Administration level only.

Procedure

To record or disable the VMUIF tutorial, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.
3	Select the VMUIF introductory tutorial for dial pulse or touch tone service.
4	Use the following table to determine the next step.

IF you want to	THEN
disable the tutorial	go to step 5.
record a custom tutorial	go to step 6.

Step	Action
5	Select None.
6	Move the cursor to the Voice/Tutorial Recorded field.
7	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
8	Type the number of the telephone you will use to make the recording, and press <Return>. **Result:** The telephone rings.
9	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
10	Select the [Record] softkey. **Result:** The [Record] softkey changes to the [Stop] softkey.

Step	Action
11	At the tone, record your tutorial.
12	To stop recording, select the [Stop] softkey. **Result:** The recording stops.
13	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 14.
record the tutorial again	select the [Delete] softkey, and go to step 10.
save the recording	go to step 15.

14	To play back the recording, select the [Play] softkey.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.
17	To enable the recording, in the Voice Messaging Options screen, move the cursor to the VMUIF Introductory Tutorial (Voice) field, and select Custom.

Recording the VMUIF login greeting

Introduction

You may prefer to customize or disable the default login greeting.

Administration level

You can customize or disable the VMUIF login greeting from the Customer Administration level only.

Procedure

To record or disable the VMUIF login greeting, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.
3	Select Login Greeting (Voice).
4	Use the following table to determine the next step.

IF you want to	THEN
disable the greeting	go to step 5.
record a custom greeting	go to step 7.

Step	Action
5	Select None.
6	Move the cursor to the Login Greeting Recorded field.
7	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
8	Type the number of the telephone from which you will make the recording, and press <Return>. **Result:** The telephone rings.
9	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
10	Select the [Record] softkey. **Result:** The [Record] softkey changes to the [Stop] softkey.

Step	Action
11	At the tone, say your greeting.
12	To stop recording, select the [Stop] softkey. **Result:** The recording stops.
13	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 14.
record the greeting again	select the [Delete] softkey, and go to step 10.
save the recording	go to step 15.

Step	Action
14	To play back the recording, select the [Play] softkey.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.
17	To enable the recording, in the Voice Messaging Options screen, move the cursor to the Login Greeting (Voice) field, and select Custom.

Chapter 7

Setting up Meridian Mail security

In this chapter

Overview	7-2
Section A: Telecommunication criminals and the problems they pose	7-3
Section B: Using Basic Access Restrictions features	7-9
Section C: Features that modify access restrictions	7-21
Section D: Controlling remote access to calling privilege	7-39
Section E: Controlling access through Least Cost Routing (BARS/NARS)	7-47
Section F: Controlling access to PBX administration programs	7-73
Section G: Controlling Direct Inward System Access	7-83
Section H: Restriction/Permission lists	7-89
Section I: Controlling access to Meridian Mail services and features	7-103
Section J: Controlling access to Meridian Mail mailboxes	7-123
Section K: Monitoring access to Meridian Mail mailboxes and features	7-149
Section L: Equipment security	7-163

Overview

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. As system administrator, it is your responsibility to take all necessary precautions to prevent security breaches. For example, unless your system has been properly secured, someone who is connected to Meridian Mail (such as a user who is logged on to a mailbox, or an external caller who has connected to Meridian Mail through a call answering session or a voice menu) can place unauthorized calls that will be billed to your system.

In this chapter

This chapter is divided into

- an overview which describes the purpose and contents of this chapter
- Section A: Telecommunication criminals and the problems they pose, which describes the types of telecommunication criminals and the problems they pose to your system
- a third part which provides information and instructions on how you can use Meridian 1 software features to control access to your switch

  This part starts at Section B: and ends at Section G:.
- a fourth part which provides information and instructions on how to use Meridian Mail security features

  This part starts at Section H: and ends at Section K:.
- Section L: Equipment security which describes how to control access to your system hardware

Section A: Telecommunication criminals and the problems they pose

In this section

Overview	7-4
Designing a security system	7-7
Ongoing security measures	7-8

Overview

Introduction

Telecom fraud has existed since the 1970s when "telephone criminals," or hackers, called their families and friends using stolen credit calling codes. By the late 1970s, hackers were using modems to access computerized systems from remote locations. By the mid-1980s, they were able to crack codes at computer speed using a personal computer with random number generating programs and autodialers.

Today, telephone operating companies are no longer the primary target for toll fraud as these companies have decreased their vulnerability by aggressively using software controls and prosecuting toll fraud criminals. For this reason, hackers trying to steal codes have migrated to new and potentially more devastating targets—customer premise equipment (for example, the PBX, Meridian Mail, and so on). Hackers are now using PBXs to place thousands of unauthorized calls primarily through inbound 800 numbers and voice mail.

What they gain

Hackers usually want one of the following:

- authorization codes which allow them to use your private branch exchange (PBX) for local and long-distance calls

  Authorization codes can then be sold or stored for future use.
- the use of your voice messaging system for their own purposes

  For example, they can use your system as a bulletin board to exchange lists of calling card numbers, coordinate illegal activities, and so on.
- to degrade your system performance

How they do it

There are several ways in which a hacker can try to access your system. The first is unauthorized access to the PBX; the second is unauthorized access to the voice messaging system, in this case, Meridian Mail; unauthorized access to personal mailboxes; and unauthorized access to the equipment.

Therefore, a good security system has to incorporate elements from PBX and system security, and awareness on the part of your users in order to provide effective security.

Unauthorized access to the PBX

Hackers are using the PBX to place unauthorized calls primarily through inbound 800 numbers and voice mail.

Nortel's Meridian 1 products meet a wide variety of customer requirements. In particular, the Meridian 1 (M1) has security features to help minimize its vulnerability while maintaining its flexibility.

For more information, see Sections B to G.

Unauthorized Meridian Mail access

Hackers may attempt to hack into your voice messaging system so they can use the outdialing feature to make free local- and long-distance calls.

With Meridian Mail, you can reduce, if not eliminate, this abuse by implementing some or all of the recommendations for system access. For more information, see Sections H to K.

Unauthorized mailbox access

Most hackers want access to the outdialing features—they are not concerned with personal mailboxes. If they do hack into a personal mailbox, they usually have some "fun" with it like changing the greeting, listening to messages, and so on.

With Meridian Mail, you can reduce the risk of unauthorized mailbox access by implementing some or all of the recommendations for mailbox access. For more information, see "Controlling access to Meridian Mail mailboxes" on page 7-123.

Unauthorized access to the equipment

Your system hardware could be a potential point of unauthorized access.

What can be done about it?

Inadequate control of calling privileges and of physical access to switching systems can cost your business millions of dollars. To secure your PBX and limit its exposure to corporate espionage and toll fraud, you need to implement security measures for

- PBX access
- Meridian Mail system access
- personal mailbox access
- equipment access

Designing a security system

Introduction

When designing a security system, consider the following two questions:

- How can you train your staff to responsibly use Meridian Mail?
- How can you prevent unauthorized use of your PBX and Meridian Mail system?

Both of these factors will help in keeping your Meridian Mail system safe from individuals who want to abuse your system.

Training your staff

Controlling access privileges to prevent PBX toll fraud and abuse of your telephone system will affect *all* employees in your organization, regardless of their positions or responsibilities. Implementing a communication program about the potential for fraud and abuse of your Meridian Mail communication system will help motivate your employees to prevent such abuse.

Ongoing security measures

Introduction

Once you have established your security practices, you should review them

- several months after the practices have been implemented so you can evaluate the results

  This will help determine if certain practices require modification.
- whenever you notice strange calling patterns

  These patterns will appear on reports listing numbers that are being called from your location or charges that are being billed to your company.

Remember to include your security practices in the orientation session for new employees.

Section B: Using Basic Access Restrictions features

In this section

Overview	7-10
Trunk Group Access Restrictions	7-11
Class of Service	7-13
TGAR/TARG and CLS interaction	7-17
Transfer feature on modems	7-19

Overview

Introduction

By providing internal and external users access only to the facilities and calling privileges that their jobs require, you can greatly decrease the potential for system abuse and toll fraud. With Basic Access Restrictions features, you can deter internal abuse and restrict external access to toll facilities.

The features

The Basic Access Restrictions features you can apply to stations, TIE trunks, and authorization codes are as follows:

- Trunk Group Access Restrictions (TGAR/TARG) controls the specific trunk groups to which a station, TIE trunk, Direct Inward System Access (DISA) directory number, or authorization code has direct access.

  For more information, see “Trunk Group Access Restrictions” on page 7-11.

- Class of Service (CLS) controls the degree of access; that is, once access is provided, CLS determines whether users can make local, TIE trunk, or long-distance calls.

  For more information, see “Class of Service” on page 7-13.

Trunk Group Access Restrictions

Introduction

Trunk Group Access Restrictions (TGAR) controls access to various trunk groups including trunks that interface with the exchange network, with TIE and CCSA networks, and with services such as paging, dictation, and recorded announcements.

How it works

Stations, TIE trunks, DISA directory numbers (DNs), and authorization codes are assigned to a group (TGAR). When users attempt to access a trunk route from a station, TIE trunk, DISA DN, or authorization code, the Meridian 1 software compares their group assignment (TGAR) against the list of denied Trunk Access Restrictions Group (TARG) associated with the trunk route they are trying to access.

If access is permitted, the Meridian 1 software then uses the Class of Service (CLS) assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when a user is trying to access trunk facilities directly.

By partitioning stations, TIE trunks, DISA DNs, and authorization codes into appropriate groups based on your corporate culture, you can stem internal abuse and external fraudulent activity, such as “looping” from PBX to PBX or to other carriers to mask the call’s origin.

Implementing and auditing the feature

Use the following table to implement or audit the TGAR/TARG feature on the Meridian 1.

For	Implement using	Print using
Stations	LD 10/11—TGAR	LD 20 by TN LD 10/11 by TN from Release 19 and up
Authorization codes	LD 88—TGAR	LD 88 by authorization code
TIE trunks	LD 14—TGAR	LD 20 by TN
Trunk groups (Route)	LD 16—TARG	LD 21 by route or access code
DISA DNs	LD 24—DISA	LD 24 by DISA DN

Class of Service

Introduction

Class of Service provides the flexibility to partition stations, TIE trunks, DISA DNs, and authorization codes into calling privilege "levels" that suit your business needs. Again, these features can inhibit internal abuse and help protect your system by preventing users from placing calls through external sources.

Class of Service restriction levels

You can assign any one of the following Class of Service restriction levels to each station, TIE trunk, and authorization code to control the degree of access to the exchange network.

- ***Unrestricted Service (UNR)*** Allowed to originate and receive calls from the exchange network.
- ***Conditionally Unrestricted (CUN)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunk but unrestricted for toll calls placed through Automatic Number Identification (ANI).
- ***Conditionally Toll-Denied (CTD)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunks, but unrestricted for toll calls placed through Basic/Network Alternate Route Selection (BARS/NARS).
- ***Toll-Denied Service (TLD)*** Allowed to receive calls from the exchange network and to dial local exchanges. Calling privileges of toll-denied stations may be modifiable through Code Restriction or New Flexible Code Restriction to allow or deny certain dialing sequences.
- ***Semi-Restricted Service (SRE)*** Allowed to receive calls from the exchange network. Restricted from all dial access to the exchange network but allowed access to TIE trunks. Allowed to access the exchange network through an attendant or an unrestricted station.

Class of Service restriction levels (cont'd)

- ***Fully Restricted Service*** Three classes of Fully Restricted Service are available:
  - ***FRE*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks, and to and from the exchange network using call modification from an unrestricted station. Denied access, either through dialing or through the attendant, to and from the exchange network.
  - ***FR1*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks. Denied access to and from the exchange network.
  - ***FR2*** Allowed to originate and receive internal calls. Denied access to TIE and CCSA networks, and to the exchange network.

Assigning a Class of Service

The following table outlines various call types and indicates whether they are possible within each Class of Service assignment.

	Class of Service assignment						
Call type	**UNR**	**CTD/CUN**	**TLD**	**SRE**	**FRE**	**FR1**	**FR2**
Incoming trunk calls	Yes	Yes	Yes	Yes	Through call modification only (see Note 1)	No	No
Outgoing non-toll trunk call	Yes	Yes	Yes	Attendant or station-extended only	Station-extended only	No	No
Outgoing toll trunk call (see Note 2)	Yes	No direct access. Yes, through BARS, NARS, or CDP if allowed through NCOS	Attendant or station-extended only		NA	No	No
Incoming/ outgoing TIE call	Yes	Yes	Yes	Yes	Yes	Yes	No
Station-to-station call	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Note 1: Call modification (transfer from station, call pickup, or transfer answer from any station) may be allowed or denied for each system.							
Note 2: A toll call to the Meridian 1 is 0+ or 1+ dialing on a central office or foreign exchange trunk.							

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Class of Service feature.

For	Implement using	Print using
Stations	LD 10/11—CLS	LD 20 by TN; LD 10/11 by TN from Release 19 and up LD81 by COS
Authorization codes	LD 88—CLS	LD 88 (by authorization code)
TIE trunks	LD 14—CLS	LD 20 by TN
Trunk groups (Route)	LD 24—CLS	LD 24 (by DISA DN)

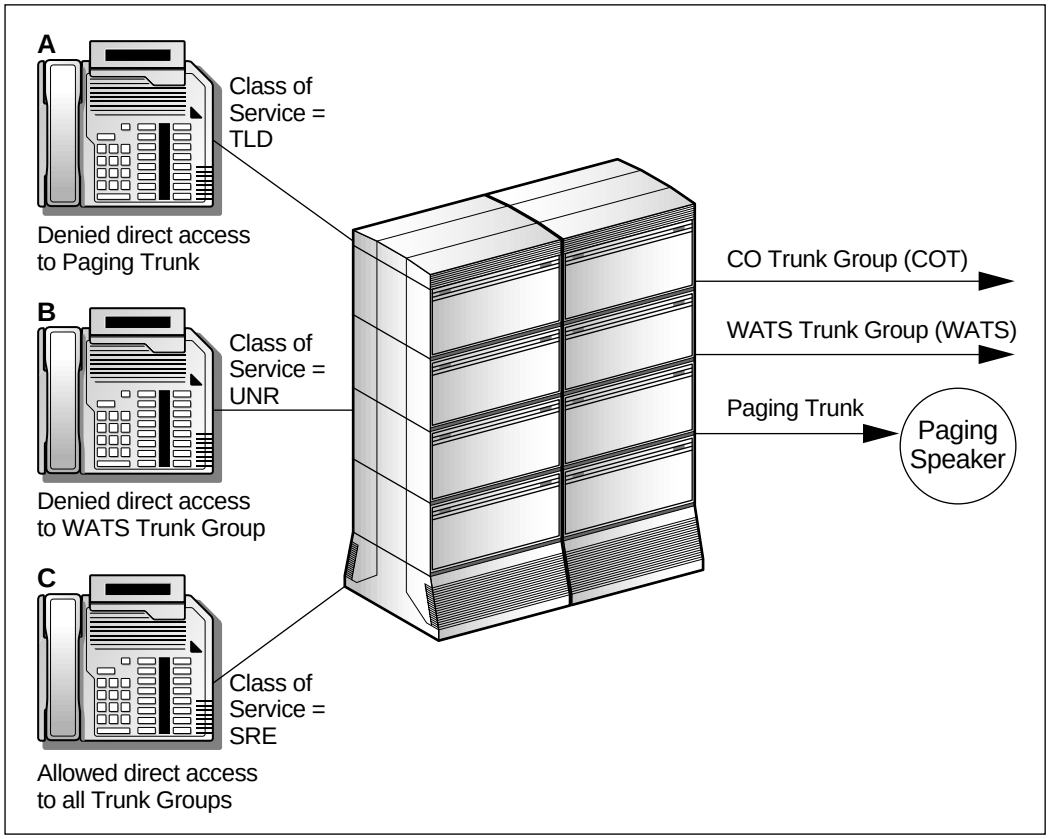
TGAR/TARG and CLS interaction

Introduction

You can use CLS and TGAR/TARG to control access to and from your trunk facilities. By assigning the most appropriate Class of Service (COS) and TGAR, you can limit your system's vulnerability to toll fraud and internal abuse.

Interaction

The following illustration shows the interaction between the Class of Service (CLS) assignment and Trunk Group Access Restrictions (TGAR).



G100446

In this illustration, the following occurs:

- User C dials access code to CO trunk group, followed by 555-6100.
- Meridian 1 checks Trunk Access Restriction Group to see if user has access to CO trunks.

  User C does.
- Meridian 1 checks CLS (SRE) to see if user can make a local call.

  User C cannot make a local call.
- Call is not allowed through CLS.

In summary, when a user attempts to access a trunk route, the Meridian 1 compares the TGAR assignment against the list of denied TARGs associated with the route that the user is trying to access. If the TARG is not listed, the Meridian 1 then uses the CLS assignment to determine call eligibility.

The system uses the most restrictive assignment, CLS or TGAR, to determine call eligibility when a user is attempting to place a call by way of direct access to trunk facilities.

Transfer feature on modems

Introduction

Hackers also use “smart” modems to infiltrate a PBX taking advantage of systems whose 2500 dataports were programmed with unnecessary features. The most common data hack is perpetrated by one “smart” modem calling another and leaving a series of instructions at the receiving modem.

How it works

The instructions require the receiving modem to emulate a switchhook flash (transfer), out pulse a series of numbers from the calling modem, and switchhook again. This effectively transfers the call back to the PBX and out again.

What you can do about it

The modem port usually has calling privileges assigned that are not required for the modem to function. Many times, a 2500-set template is used that is also used for single-line phones. Frequently, the administrator is unaware that the 2500 port will be used for data,

Modem phones should be identified and the transfer feature removed if possible. The default on 2500 sets is “deny.” Be sure the class of service, TGAR, and NCOS do not allow long-distance calling whenever possible.

Section C: Features that modify access restrictions

In this section

Overview	7-22
System Speed Call	7-23
Authorization Codes	7-24
Station Specific Authorization Codes	7-25
Forced Charge Account	7-27
Controlled Class of Service	7-29
Enhanced Controlled Class of Service	7-32
Flexible Feature Codes—Electronic Lock	7-33
Code Restriction	7-34
New Flexible Code Restriction	7-36

Overview

Introduction

The following features can be used to selectively override Class of Service (CLS) and Trunk Group Access Restrictions (TGAR) when you need to extend a station's or TIE trunk's normal calling capabilities:

- System Speed Call

  For more information, see "System Speed Call" on page 7-23.
- Authorization Code

  For more information, see "Authorization Codes" on page 7-24.
- Station Specific Authorization Code

  For more information, see "Station Specific Authorization Codes" on page 7-25.
- Forced Charge Account

  For more information on, see "Forced Charge Account" on page 7-27.
- Controlled Class of Service

  For more information, see "Controlled Class of Service" on page 7-29.
- Enhanced Controlled Class of Service

  For more information, see "Enhanced Controlled Class of Service" on page 7-32.
- Flexible Feature Codes—Electronic Lock

  For more information, see "Flexible Feature Codes—Electronic Lock" on page 7-33.
- Code Restrictions

  For more information, see "Code Restriction" on page 7-34.
- New Flexible Code Restriction

  For more information, see "New Flexible Code Restriction" on page 7-36.

System Speed Call

Introduction

System Speed Call extends the capabilities of the Speed Call feature. In addition to providing abbreviated dialing, using an entry in a System Speed Call list lets the internal user temporarily override the Class of Service and TGAR assigned to a station, and place a call to a telephone number in the System Speed Call list.

How it works

With this feature, you can assign the most appropriate CLS and TGAR restrictions to a station to limit the potential for unauthorized calling, and, at the same time, allow calls to approved destinations. The "approved telephone numbers" that you define in a system Speed Call list extend the station's calling privileges beyond the station restriction levels.

You can assign stations to different System Speed Call lists. You can also designate these stations as either System Speed Call Users (SSUs) or System Speed Call User/Controllers (SSCs) of the list. You can also assign list controlling capabilities to a key on the attendant console. However, this key cannot override CLS and TGAR because the attendant is not subject to these restrictions.

Note: A System Speed Call list can also override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the System Speed Call feature.

For	Implement using	Print using
Stations	LD 10—FTR LD11—SSU, KEY	LD 20 by TN; LD 10/11 by TN from Release 19 and up LD81 by SSU, SSC, KEY
Speed Call list	LD 18—SSC, all prompts	LD 20 by list number
Attendant	LD 12—KEY	LD 20 by TN

Authorization Codes

Introduction

Authorization codes allow users to place business calls from stations normally restricted from doing so. These restricted stations may be located in areas of public access or used by employees who do not require broader calling privileges.

How it works

Authorization codes enable selected users to temporarily override the access restrictions assigned to a station or a TIE trunk. A user enters an authorization code which has an associated Class of Service (CLS), TGAR, and Least Cost Routing or Network Class of Service (NCOS). The user has the calling privileges of the authorization codes rather than those of the station or TIE trunk for the duration of the call.

Considerations

When you implement the Authorization Code feature, you should consider making the authorization codes as long as your corporate culture will allow, assigning unique authorization codes to each user, and allowing calling privileges based on user requirements.

You can also output the codes as part of the Call Detail Records (CDR) to look for call patterns that indicate possible unauthorized access or abuse. You should design and implement procedures for assigning authorization codes to new employees and for deleting codes that are no longer valid because of attrition or abuse.

Note: You may use authorization codes to override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Authorization Codes feature.

For	Implement using Overlay programs/features prompts	Print using Overlay programs
Authorization codes	LD88—all prompts	LD 88 by authorization code

Station Specific Authorization Codes

Introduction

The Station Specific Authorization (Authcode) Code is offered in X11 Release 19 as a separate package. It allows you to define the authorization code access level of a set.

How it works

The Station Specific Authorization Code feature is implemented on a per set basis. The system will cross-check between overlays 10, 11, and 88 to ensure that the authorization code being used is valid. The only time cross-checking is not performed is when authorization codes are deleted from overlays 10 or 11. You must remove the authorization codes from overlay 88 as well as overlays 10 or 11.

Levels of access

There are three levels of authorization code access:

- ***Authcode Unrestricted (AUTU)*** A set programmed AUTU will be allowed to enter any authorization code without additional restrictions.
- ***Authcode Restricted (AUTR)*** When a set is configured AUTR, the authorization code entered by the user must match one of the preassigned authorization codes. Any other authcode will be treated as invalid, and an error message will be generated at the TTY.
- ***Authcode Denied (AUTD)*** No authorization code entry will be accepted for a set configured as AUTD.

Implementing and auditing

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Station Specific Authorization Codes feature.

For	Implement using	Print using
LD 10/11 stations	LD 10/11 (AUTU), AUTR, AUTD MAUT YES/NO SPWD (prompted if MAUT=YES) AUTH	LD 20 by TNB LD 10, 11 by TNB from Release 19 and up
LD 81 ODAS	LD 81 FEAT AUTU, AUDT, AUTD	LD 81 by FEAT
LD 88 Authorization Code	LD 88 AUTH	LD 88 by AUTH

Forced Charge Account

Introduction

With Forced Charge Account (FCA), the system forces the user to act before greater calling privileges are granted.

How it works

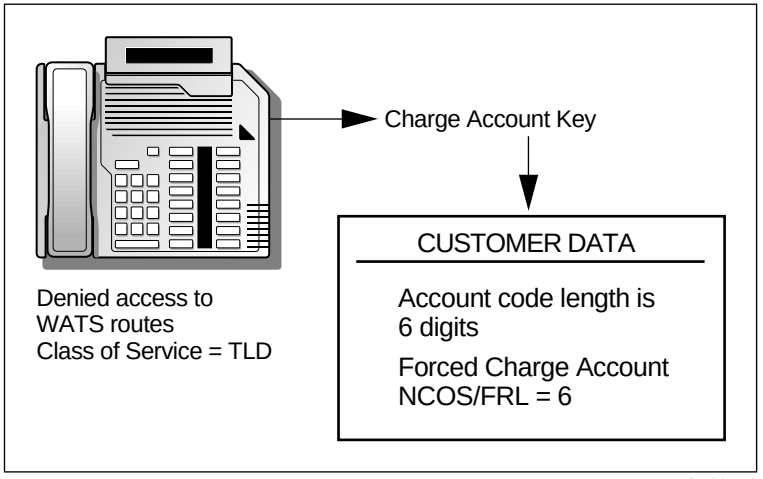
The Forced Charge Account feature temporarily overrides the toll-denied Class of Service Restriction (TLD) provided the user enters an account code before placing a toll call. After the user enters an account code, the Meridian 1 software checks only for a valid account code length—not for valid digits within an account code. Once the Meridian 1 verifies the account code length, the user has an unrestricted Class of Service or the customer-defined Forced Charge Account Network Class of Service (NCOS), or both, for the duration of the call.

The Call Detail Recording (CDR) software outputs a charge record which identifies the charge account used for the call.

Note: You can use the Forced Charge Account feature to override the restrictions imposed through the Least Cost Routing software.

Example

The following illustration is an example of how Forced Charge Account works.


Charge Account Key
CUSTOMER DATA
Account code length is 6 digits
Forced Charge Account NCOS/FRL = 6
Denied access to WATS routes
Class of Service = TLD

G100450

Example, cont'd

In this example, the following takes place:

- User goes off-hook to obtain a dial tone.
- User presses Charge Account key.
- User dials six-digit account code.
- Account code record is generated in CDR.
- User receives a dial tone and dials a number in the normal manner.
- Set becomes UNR (unrestricted) for this one call.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Forced Charge Account feature.

For	Implement using	Print using
Customer	LD 15—CHLN, FCAF, CHMN, FCNC	LD 21 by CUST, by CDR from Release 19 and up
Stations	LD 10/11—TLD, FCAR	LD 10, 11 by TN from Release 19 and up LD 20 by TN
TIE trunks	LD 14—TLD, FCAR	LD 20 by TN

Controlled Class of Service

Introduction

You can use Controlled Class of Service to lower calling privileges of sets in unsecured areas and still raise their calling privileges when required. This feature is particularly effective in preventing internal abuse.

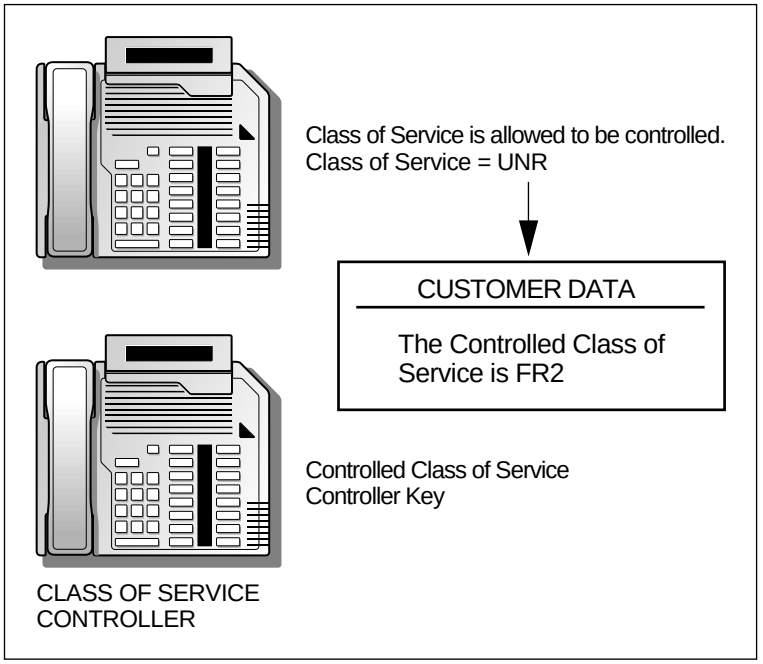
How it works

The Controlled Class of Service (CCOS) feature allows users of SL-1 and Meridian digital sets designated as controllers, and users of TTYs designated as background terminals, to temporarily alter a designated station's Class of Service assignments (CLS). When a station is in the controlled mode, its CLS is derived from the Controlled Class of Service restriction level defined for each customer.

Users of SL-1 and Meridian digital sets designated as controllers can place stations in a controlled mode one at a time whereas background terminals can alter individual, group, or all designated stations at one time.

Example

The following illustration is an example of how the Controlled Class of Service feature works.


Class of Service is allowed to be controlled.
Class of Service = UNR
CUSTOMER DATA
The Controlled Class of Service is FR2
Controlled Class of Service Controller Key
CLASS OF SERVICE CONTROLLER
G100451

In this example, the controller does the following:

- presses the Controller key
- dials the directory number of the set to be controlled
- presses the Controller key.

  The set is now an FR2 Class of Service

To return that set to the UNR Class of Service, the controller presses the Controller key, dials the DN for the set, and presses the Controller key again. The set will be reset to a UNR Class of Service.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS	LD 21 by CUST or by CCOS
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN
Stations to be controllers	LD 11—KEY	LD 20 by TN LD 81 CCOS Key
Background terminals	LD 17—ADAN, USER	LD 22 by CFN, ADAN from Release 19 and up

Enhanced Controlled Class of Service

Introduction

This enhancement expands the Controlled Class of Service feature to further control calling privileges of stations in unsecured areas. Enhanced Controlled Class of Service (ECCS) extends the controller function of Controlled Class of Service (CCOS) to attendant consoles and the M3000 sets equipped with a Controller key. In addition, this enhancement allows for two more customer-defined levels of CCOS restriction.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Enhanced Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS, ECC1, ECC2	LD 21 by CUST or by CCOS from Release 19 and up
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN
Stations to be controllers	LD 11—KEY	LD 11 by TN from Release 19 and up LD 20 by TN LD 81 CCOS Key
Attendants to be controllers	LD 12—KEY	LD 20 by TN LD 81 CCOS key
Background terminals	LD 17—USER	LD 22 by CFN, by ADAN from Release 19 and up

Flexible Feature Codes—Electronic Lock

Introduction

Electronic Lock (ELK) allows selected users to activate and deactivate the Controlled Class of Service (CCOS) mode from their stations by entering the Station Control Password (SCPW) and the appropriate Electronic Lock code.

Station users can activate the Electronic Lock feature to prevent unauthorized calls from their sets when they are not able to control physical access. The feature is used typically in the evenings or on weekends.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Electronic Lock feature.

For	Implement using	Print using
Customers	LD 15-CCRS, SCPL	LD 21 by CUST or by CCOS from Release 19 and up
Flexible Feature code	LD 57—FFCT, CODE, ELKA, ELKD	LD 57
Stations	LD 10/11—SCPW, CLS	LD 10/11 by TN from Release 19 and up LD 20 by TN

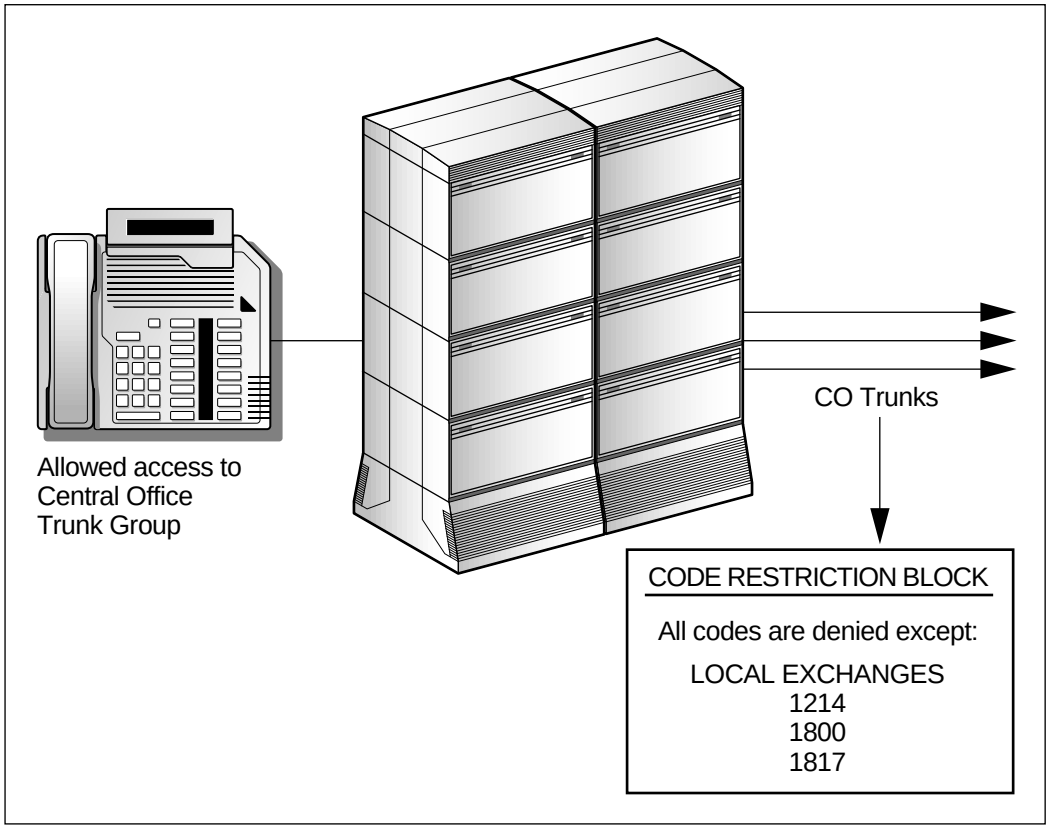
Code Restriction

Introduction

The Code Restriction feature allows toll-denied stations, TIE trunks, DISA DNs, and authorization codes limited access to the toll-exchange network—that is, to CO and FX trunks. For each CO and FX trunk group, you can build a code restriction block that specifies the allowed area codes and exchange codes for toll-denied users accessing those facilities.

Example

The following illustration is an example of how the Code Restriction feature works.



G100452

Example (cont'd)

In this example, the following takes place:

- The user goes off-hook and dials the access code for CO trunks followed by 1-800-555-0110.
- The station is TLD and not normally allowed to dial 1+, but a code restriction is in effect.
- Meridian 1 checks the Code Restriction Table for CO trunks and finds that 1-800 is allowed.
- The call is completed.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Code Restriction feature.

For	Implement using	Print using
Code Restriction	LD 19 all prompts	LD 21 by CRB
Stations	LD 10/11—CLS=TLD	LD 10/11 by TN from Release 19 and up LD 20 by TN LD 81 by TLD

New Flexible Code Restriction

Introduction

To extend the calling privileges normally associated with toll-denied Class of Service, New Flexible Code Restriction allows you to partition toll-denied users into groups. Each toll-denied group can have unique calling privileges. New Flexible Code Restriction (NFCR) enhances Code Restriction by letting you selectively allow or deny toll-denied stations, TIE trunks, DISA DNs, and authorization codes to make certain calls on outgoing trunk routes. With New Flexible Code Restriction, the Meridian 1 determines whether the toll-denied user can make a call on a specific trunk route by checking the specific digit sequence dialed, the number of digits dialed, or both.

How it works

You can assign toll-denied users to a Network Class of Service (NCOS) and allow or deny calling privileges according to the Facility Restriction Level (FRL) of the NCOS. Toll-denied stations, TIE trunks, and authorization codes can be assigned from 1 to 100 possible NCOS groups. Each NCOS group can be assigned to one of eight possible FRLs.

When the toll-denied user accesses an outgoing route, the Meridian 1 compares the FRL of the user's NCOS to a table that defines the calling privileges associated with that trunk group.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the New Flexible Code Restriction feature.

For	Implement using	Print using
Customer	LD 15—NFCR, MAXT	LD 21 by CUST or by ESN from Release 19 and up
Network control	LD 87—NCOS, FRL	LD 87 by NCOS
New Flexible Code Restriction block	LD 49-FCR for all prompts	LD 49 FCR
Route	LD 16—FRL	LD 21 RDB
Station	LD 10/11—NCOS, CLS=TLD	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by COS, NCOS
DISA	LD 24—NCOS	LD 24 by DISA DN

Section D: Controlling remote access to calling privilege

In this section

Overview	7-40
Call Forward All Calls	7-41
Call Forward External Deny	7-42
Call Forward to Trunk Access Code—DID Calls	7-43
Internal Call Forward	7-44
Flexible Feature Codes—Remote Call Forward	7-45
User Selectable Call Redirection	7-46

Overview

Introduction

Two of the most commonly abused features are Call Forward All Calls and Direct Inward System Access (DISA).

Call Forward

Call Forward is a convenient feature that allows users who are going to be away from their desks to forward their calls to another set or location.

Call Forward All Calls

The Call Forward All Calls feature is assigned on a per station basis and designates the maximum number of digits to which a user may call forward. DISA allows users in remote locations to place calls through your corporate PBX.

Types of abuse

Station users have abused Call Forwarding by forwarding their sets to either a long-distance telephone number or to a trunk access code, then going offsite, and making a call to their sets. With the introduction of Remote Call Forward, non-users can abuse Call Forward if proper controls are not in place.

In this section

This section describes additional controls you can use with the Call Forward features to stem abuse and unauthorized calls.

Call Forward All Calls

Description

Call Forward (CFW) allows users to forward all calls manually to another number either internal or external to the system. The ability to forward a phone outside the system depends not only on the number of digits assigned to the call forward feature, but on the assignment of the feature Call Forward External Allow, also assigned on a phone-by-phone basis.

What you should look for

The default for CFW is 16, adequate for many international calls. Ensure this feature is restricted to the minimum in all cases (usually four—the standard number of digits in an extension). Be aware of the combinations of external forwarding and long digit strings allowed. Permit only where absolutely necessary.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward All Calls feature.

For	Implement using	Print using
Stations	LD10, 11—CFW	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by CFW

Call Forward External Deny

Description

This feature provides the option to restrict, on a set-by-set basis, the ability to call forward all calls to an external directory number (DN).

With Release 19, the default value for Call Forward External becomes “deny.”

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward External Deny feature.

For	Implement using	Print using
Stations	LD 10, 11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by CFXA, CFXD

Call Forward to Trunk Access Code—DID Calls

Description

You may not want your users to call forward their stations to an access code. After all, an unrestricted station forwarding to the central office trunk (COT) access code puts a whole world of calling capabilities at the caller's fingertips. Call Forward to Trunk Access Code provides you with the option to restrict, on a customer-by-customer basis, the ability to call forward direct in dial (DID) calls to a trunk access code.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward to Trunk Access—DID calls feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by customer

Internal Call Forward

Description

Internal Call Forward (ICF) is available for systems using X11 software Release 19 and up. ICF directs all internal calls to a specified location different from the call forward destination of external calls. An internal call is considered an extension-to-extension call, Direct Inward System Access (DISA) call, Group Call, a call over a trunk route designated as internal, an incoming trunk call using private numbering, or an attendant-originated call. The default for this feature is 4 digits but can be defined for up to 23 digits.

How to use ICF

Ensure that Call Forward to Trunk Access Codes is set to "no" in the customer Data Block and that Call Forward External is denied. A combination of these features in the "allow" state would permit users to call forward their phones to BARS/ NARS access codes or trunk access codes, and receive a second dial tone when looping through private networks or entering the system through DISA.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Internal Call Forward feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by customer
Stations	LD 10—FTR, ICF	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by ICF
Flexible Feature Codes	LD 57—ICFA, ICFD, ICFV	LD 57 by CODE

Flexible Feature Codes—Remote Call Forward

Description

The Remote Call Forward feature (RCFW) allows a user to activate and deactivate the Call Forward All Calls feature from a remote station.

How RCFW works

Users enter codes to activate and deactivate the feature, and must also enter a station-specific password. You can selectively provide this capability to users as job functions require. The user can also activate this feature from an offsite location by using DISA.

Exercise care in assigning this capability to minimize opportunities for abuse.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Remote Call Forward feature.

For	Implement using	Print using
Customer	LD 15—SCPL	LD 21 by CUST or by CFCO from Release 19 and up
Flexible Feature Code	LD 57—CODE, RCFA, RCFD, RCFV	LD 57 by FFC
Station	LD 10/11—SCPW	LD 21 by TN
DISA	LD 24 by DISA	LD 24 DISA by DN

User Selectable Call Redirection

Introduction

Release 19 introduces the ability to user-select the destination for Forward No Answer, Busy Hunt, External Forward No Answer, and External Hunt. The feature is controlled by Flexible Feature Code, Special Prefix Code, or a User key on a multiline phone.

This feature requires a Station Control Password.

Ensure that the SCPW is unique for each phone with the feature allowed.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the User Selectable Call Redirection feature.

For	Implement using	Print using
LD 10/11 SETS	LD 10 SCPW, CLS, USRA	LD 10, 11 by TN, DN from Release 19 and up LD 20 by TN LD 20 by DN
LD 15 CDB	LD 15 SPCL, FFCS	LD 21 by CUST, by CFW from Release 19 and up
LD 57 FFC	LD 57 USCR	LD 57 by CODE LD 81 by CODE

Section E: Controlling access through Least Cost Routing (BARS/NARS)

In this section

Overview	7-48
Supplemental Digit Recognition	7-50
Supplemental Digit Restriction	7-52
Network Class of Service—Facility Restriction Level	7-55
Network Speed Call	7-58
Network Authorization Code	7-60
Authorization Code Conditionally Last	7-61
Time-of-Day Routing	7-64
Routing Control	7-67
Incoming Trunk Group Exclusion	7-70

Overview

Introduction

Basic Alternate Routing System (BARS) and Network Alternate Routing System (NARS) software allows you to route outgoing calls over the least expensive facility available at the time the user places the call. You can use the BARS/NARS feature to prevent calls to a specific area code or exchange, or to international locations.

How BARS and NARS work

When the user dials an access code followed by the desired number, the software processes and routes the call. Based on the number the user dials, the Meridian 1 system reads a digit translation table. The translation determines which list of alternate routes the system will use to process the call. This list is called a route list index and contains alternate outgoing routes (trunk groups) for call completion.

Because the majority of toll-fraud calls terminate in the 809 area code and in international locations such as Egypt, Pakistan, and Columbia, consider not defining these codes in your translation tables if your business does not require that users call these locations. If your corporate culture requires calls to destinations associated with fraud, you should consider assigning unique route list indexes to each of these destinations. Such a scheme provides the capability to assess normal call volumes and detect variations.

Assessment tools

Statistics are available to indicate the number of calls placed through each route list index. It is TFN001.

Available features

The following features are elements of BARS/NARS which allow you flexibility in restricting calling privileges:

- Supplemental Digit Recognition
- Supplemental Digit Restriction
- Network Class of Service—Facility Restriction Level
- Network Speed Call
- Network Authorization Code
- Authorization Code Conditionally Last

Available features (cont'd)

- Time-of-Day Routing
- Routing Control
- Incoming Trunk Group (TIE) Exclusion

BARS/NARS features to control access privileges

The following table lists the features you should consider implementing depending on the requirements of your business.

If your business requirement is to	Then we recommend you
totally deny an area code or a local exchange	do not define them in the translation table. Calls to those numbers attempted through BARS/NARS are blocked.
deny all access to certain country codes, or exchanges within an area code	use the Supplemental Digit Restriction feature or Translation Data Block. For more information, see "Supplemental Digit Restriction" on page 7-52.
inhibit the use of certain trunk groups	use the Network Class of Service (NCOS) Facility Restriction Level (FRL) and also (optionally) Trunk Group Access Restriction (TGAR) feature. For more information, see "Network Class of Service—Facility Restriction Level" on page 7-55 and "Trunk Group Access Restrictions" on page 7-11.
deny access to certain trunk groups or destinations at a specific time	use the Time-of-Day Routing feature. For more information, see "Time-of-Day Routing" on page 7-64.
deny access to certain destinations after business hours, on weekends and holidays, or at other selected times.	use the Routing Control feature. For more information, see "Routing Control" on page 7-67.
deny calls to certain dialing sequences when those calls originate on TIE trunks	use the Incoming Trunk Group Exclusion. For more information, see "Incoming Trunk Group Exclusion" on page 7-70.

Supplemental Digit Recognition

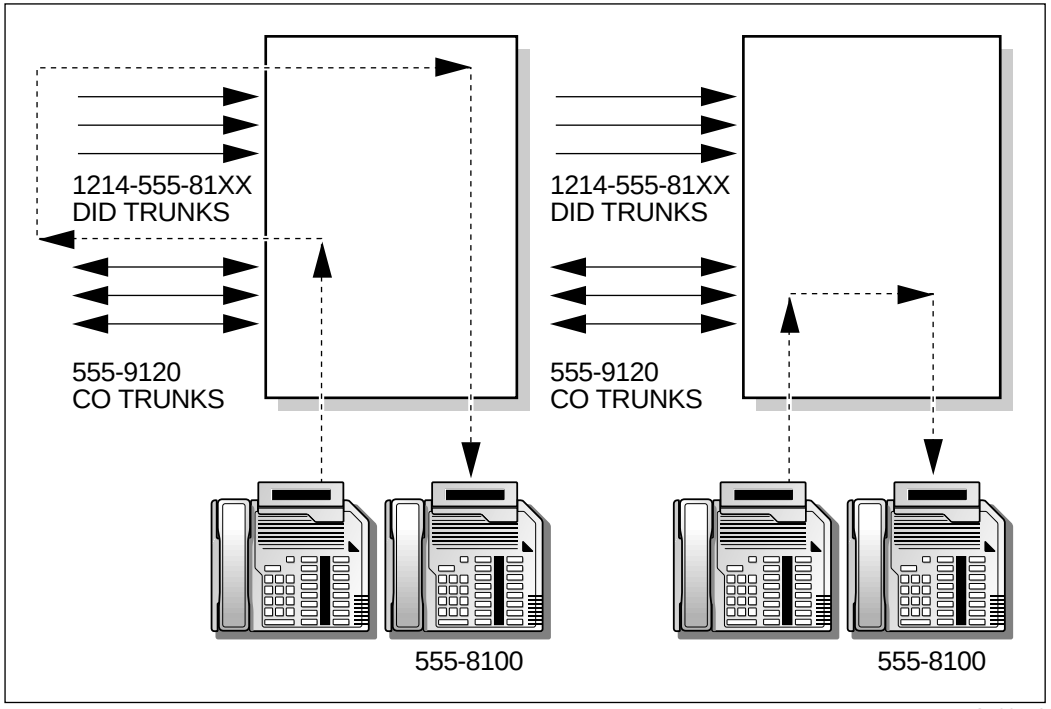
Description

One type of internal abuse or misuse occurs when callers use incoming TIE trunks. Callers on TIE trunks sometimes dial the BARS/NARS access code followed by the whole telephone number of an internal station.

When using Supplemental Digit Recognition, the Meridian 1 "recognizes" dialing sequences associated with internal calls, and thus prevents callers from using two trunks to complete an internal call.

Example

The following figure illustrates how the Supplemental Digit Recognition feature works.



G100453

Example (cont'd)

In this example, the following takes place:

- User A dials 9-555-8100.

  Meridian 1 is not programmed to recognize 555-8100 as an internal number.

  The call is routed out over a CO trunk group and is returned to the Meridian through the DID trunk group. An internal call now requires two trunks to be complete.
- User B dials 9-555-8100.

  Meridian 1 is programmed to recognize 555-8100 as an internal number and deletes 555. Meridian 1 dials 8100. The call is completed internally.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Recognition feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Supplemental Digit Restriction

Description

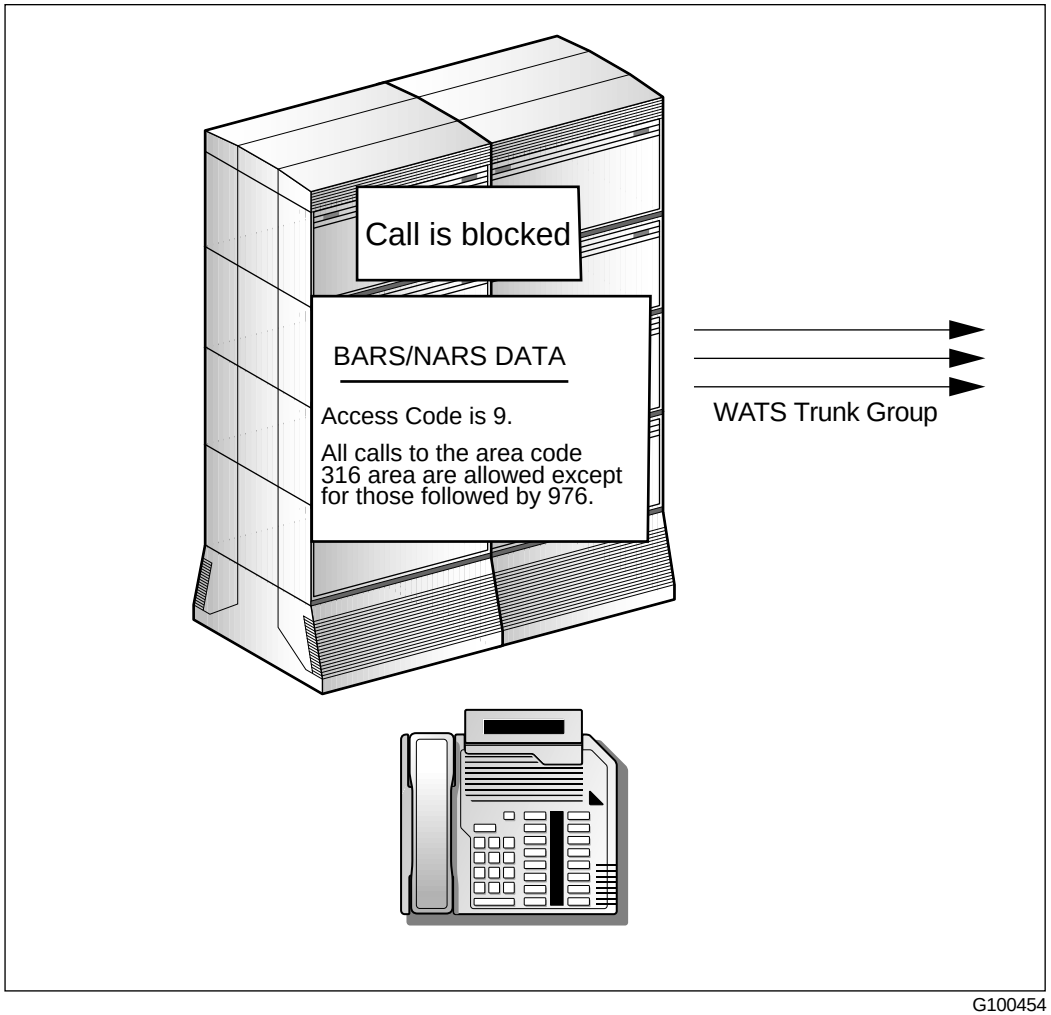
Because most toll-fraud calls are placed to international locations, you can use Supplemental Digit Restriction (SDR) to block calls to international locations that your users do not need to call.

How SDR works

Supplemental Digit Restriction enables you to block calls to certain telephone numbers within exchanges, area codes, or country codes. For example, you may have legitimate international calling requirements to many countries but none to those countries typically associated with fraud. Supplemental Digit Restriction lets you block calls to those countries.

Example

The following figure illustrates how the Supplemental Digit Restriction feature works.


Call is blocked
BARS/NARS DATA
Access Code is 9.
All calls to the area code 316 area are allowed except for those followed by 976.
WATS Trunk Group

G100454

In this example, the following takes place:

- The user dials 9-1-316-976-9090.
- The 9 triggers the Meridian 1 to use BARS/NARS data.
- Meridian 1 checks the Translation Table for 1316 and finds that 1316, followed by 976, is blocked.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Restriction feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Network Class of Service—Facility Restriction Level

Description

A Network Class of Service (NCOS) designation is a group of calling privileges you can assign to a station, TIE trunk, DISA DN, or authorization code.

How NCOS works

The Meridian 1 system uses the NCOS to determine caller treatments and eligibility for outgoing calls that use the Least Cost Routing (BARS/NARS) software. By partitioning stations, TIE trunks, DISA DNs, and authorization codes into unique NCOS groups, you can track the normal calling patterns of each group (TFN002). You can then promptly detect variances which can indicate fraudulent activity, and take action.

Within the NCOS, you can assign the user to one of eight Facility Restriction Levels (FRL). The FRL is compared to the minimum FRL requirement assigned to each entry in a route list. The entries in the route list are trunk routes that are able to place calls to the NPA, NXX, or special number. The routes are listed in the order the system searches them when trying to complete an external call. Callers are eligible to complete a call on an entry in the route list when their FRL is equal to, or higher than, the entry's FRL level.

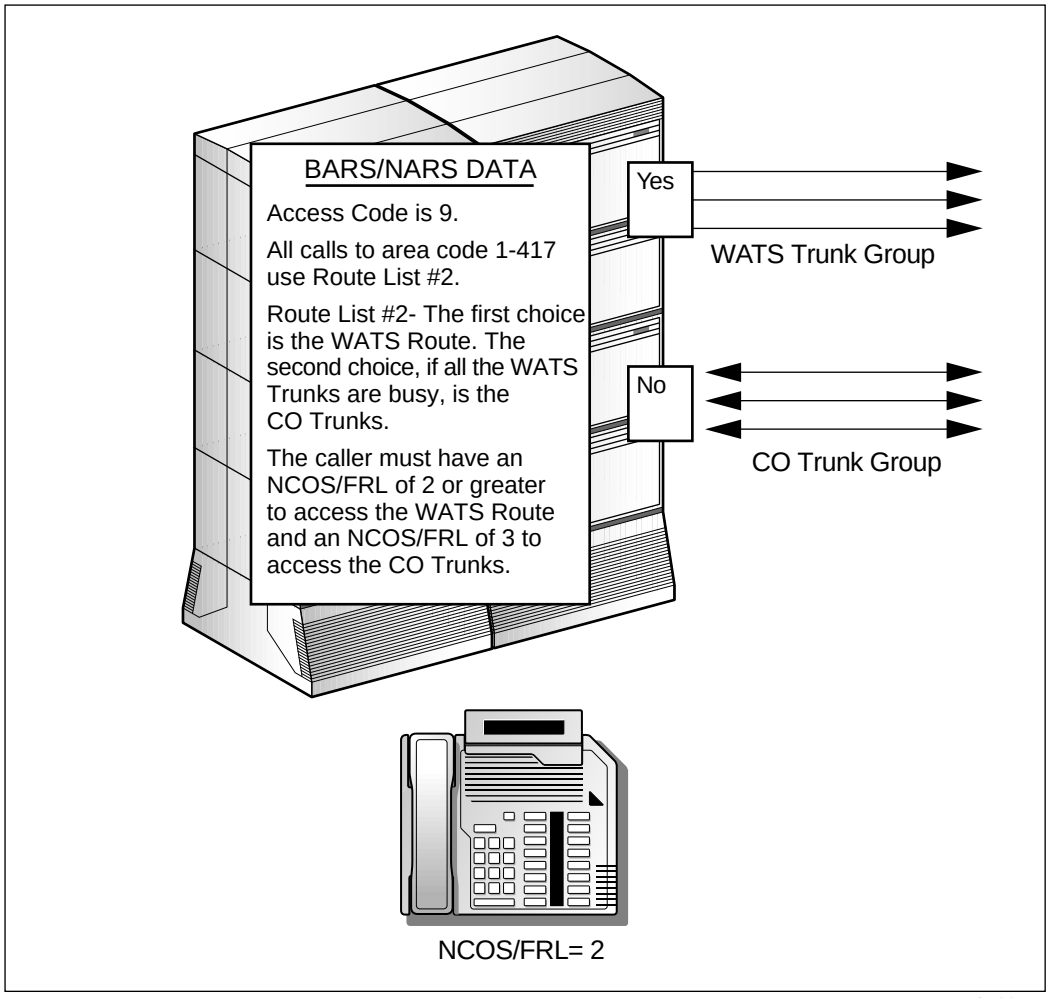
In conjunction with TGAR

The BARS/NARS database can be configured to ignore Trunk Group Access Restrictions (TGAR) or to use them. When TGARs are ignored, the BARS/NARS software assesses the Class of Service and the FRL to determine which call facilities are eligible for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls through BARS/NARS. You can base trunk access for each call on the FRL requirements for the number dialed rather than basing it on the TGAR.

You can also configure the BARS/NARS database to assess TGAR assignments in determining how the system can route a call. In this case, the BARS/NARS software will use the COS, TGAR, and FRL to determine which call facilities are eligible to process a particular call.

Example

The following illustration shows how the NCOS Facility Restriction Level feature works.


BARS/NARS DATA
Access Code is 9.
All calls to area code 1-417 use Route List #2.
Route List #2- The first choice is the WATS Route. The second choice, if all the WATS Trunks are busy, is the CO Trunks.
The caller must have an NCOS/FRL of 2 or greater to access the WATS Route and an NCOS/FRL of 3 to access the CO Trunks.
Yes
WATS Trunk Group
No
CO Trunk Group
NCOS/FRL= 2

G100454

In this example, the following occurs:

- The user dials 9-1-417-555-9090.
- The 9 triggers Meridian 1 to use BARS/NARS data.
- The Meridian 1 searches the Translation Table for 1417.
- Calls to 1417 use Route List Index 2.
- Route List Index 2 is searched for an idle available trunk.

- The first choice is the WATS route.
- The NCOS/FRL assigned to the first choice (2) is compared to the NCOS/FRL (2) of the station.
- The station's NCOS/FRL (2) is equal to, or greater than, the WATS NCOS/FRL (2), so the call is allowed for this choice.
- If all WATS trunks are busy, then the second choice (CO trunks) is checked.
- The NCOS/FRL of the CO trunks (3) is compared to the NCOS/FRL of the station (2).
- The station's NCOS/FRL (2) is lower than the CO trunks' NCOS/FRL (3), so the call cannot be completed over CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the NCOS Facility Restriction Level feature.

For	Implement using	Print using
Network control	LD 87—NCTL all prompts	LD 87 FEAT=NCTL by NCOS
Route list index	LD 86—RLB, FRL	LD 86 FEAT=RLB
Authorization code	LD 88—AUT, NCOS	LD 88 TYPE=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call list	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Speed Call

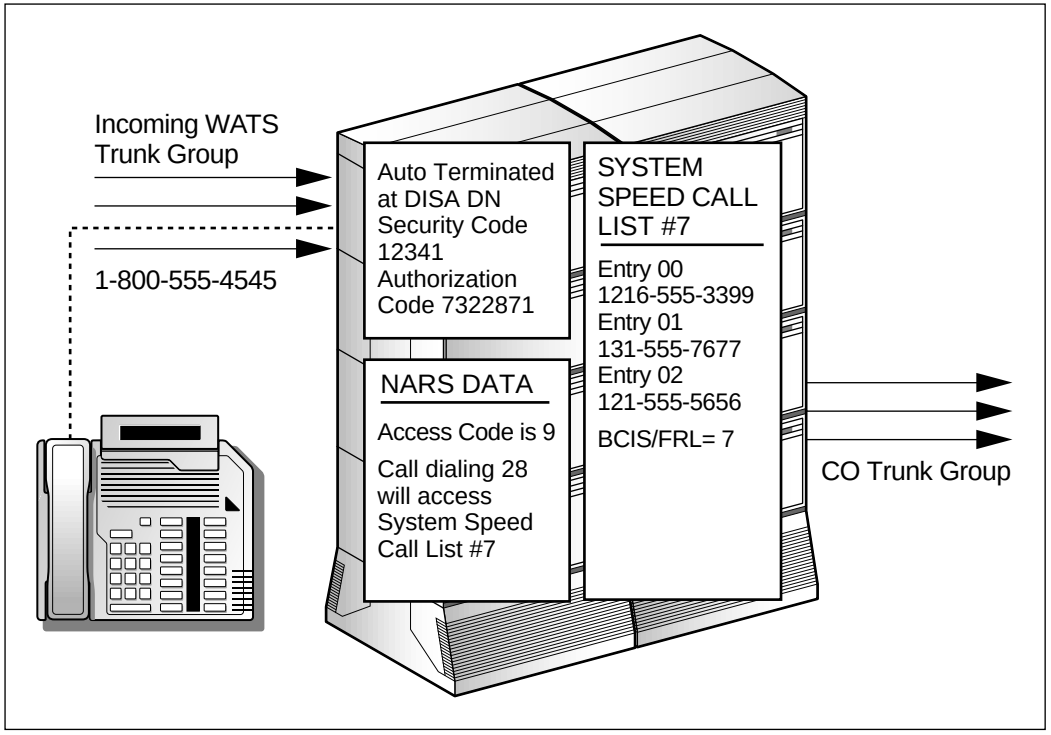
Description

You can enable a user who is normally restricted from making certain types of BARS/NARS calls, to make such a call if the destination is a company-approved number defined in a System Speed Call list. Network Speed Call expands the System Speed Call feature by allowing users to access the System Speed Call feature from the public and private networks.

You can use the Network Speed Call feature in conjunction with a restricted DISA DN. The incoming DISA caller can gain access to approved destinations through the Network Speed Call list.

Example

The following illustration shows how the Network Speed Call feature works.



G100455

Example (cont'd)

In this example, the following occurs:

- The caller dials 1-800-444-4545.
- When dial tone is returned, the user dials 12341.
- When dial tone is returned, the user dials 167322871
- When dial tone is returned, the user dials 9-20-00 to access System Speed Call Number 7.
- 9 triggers the Meridian 1 to use NARS data.
- Meridian 1 checks the Translation Table for 20 and finds 20 to be the Access Code for System Speed Call List 7.
- System Speed Call List is checked for entry 00.
- The call completes to 1-216-555-3399 based on the calling capabilities of NCOS/FRL 7.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Network Speed Call feature.

For	Implement using	Print using
Network translation	LD 90—NSCL all prompts	LD 90 AC1 or AC2, SSCL
System Speed Call	LD 18—SSC all prompts	LD 20 by SCL
Network control	LD 87—NCTL, NSC, LIST	LD 87 by NCOS
Authorization code	LD 88—AUT, NCOS	LD 88 by AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	DL 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Authorization Code

Description

With the Network Authorization Code feature, you can assign up to 20 000 authorization codes of up to 14 digits each, and you have the option of requiring users to enter an authorization code before certain calls can be processed. You may want to use this requirement for certain locations typically associated with unauthorized access like the 809 area code.

Authorization Code Conditionally Last

Introduction

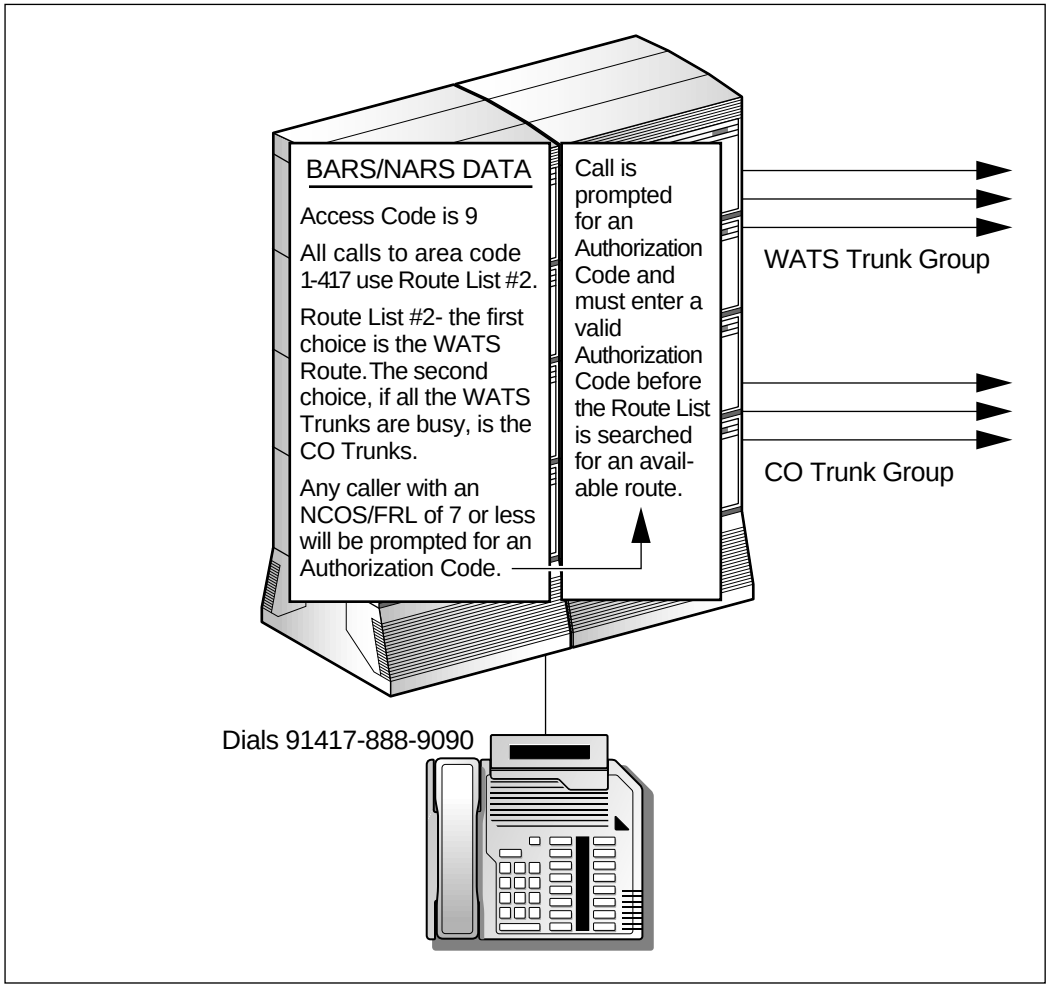
The system can prompt users “conditionally” for an authorization code after they attempt to place a call using the BARS/NARS call processing software. Users who fail to meet the minimum Facility Restriction Level requirement assigned to a route list will hear tones or a recorded announcement indicating that they need to enter an authorization code.

How this feature works

Users must enter a valid authorization code at that point to complete the call. This control provides another level of security by requiring all callers placing calls to international locations or selected area codes, for example, to enter an authorization code.

Example

The following illustration shows how the Authorization Code Conditionally Last feature works.


BARS/NARS DATA
Access Code is 9
All calls to area code 1-417 use Route List #2.
Route List #2- the first choice is the WATS Route. The second choice, if all the WATS Trunks are busy, is the CO Trunks.
Any caller with an NCOS/FRL of 7 or less will be prompted for an Authorization Code.
Call is prompted for an Authorization Code and must enter a valid Authorization Code before the Route List is searched for an available route.
WATS Trunk Group
CO Trunk Group
Dials 91417-888-9090

G100456

In this example, the following takes place:

- The user dials 9-1417-555-3376.
- 9 triggers the Meridian 1 to use the BARS/NARS data.
- The Meridian 1 checks the Translation Table for 1417 and sends calls to Route List Index 2.
- The system checks Route List Index 2 for the minimum NCOS/FRL required; it is found to be 7.

Example (cont'd)

- The NCOS/FRL of 7 is compared to the user's NCOS/FRL, in this case 2.
- Because the user's NCOS/FRL is equal to or lower than the minimum NCOS/FRL for the route list, the user is prompted for an authorization code.
- The user must enter a valid authorization code before the call can be completed. The calling capabilities of the authorization code's NCOS/FRL will determine call eligibility.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Authorization Code Conditionally Last feature.

For	Implement using	Print using
Authorization code	LD 88—all prompts	LD 88 by AUT
Route List Index	LD 86—RLB MFRL	LD 86 by RLB
Network Control	LD 87 —NCTL, NCOS FRL	LD 87 by NCOS
Authorization Code	LD 88—AUT CODE, NCOS	LD 88=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Time-of-Day Routing

Description

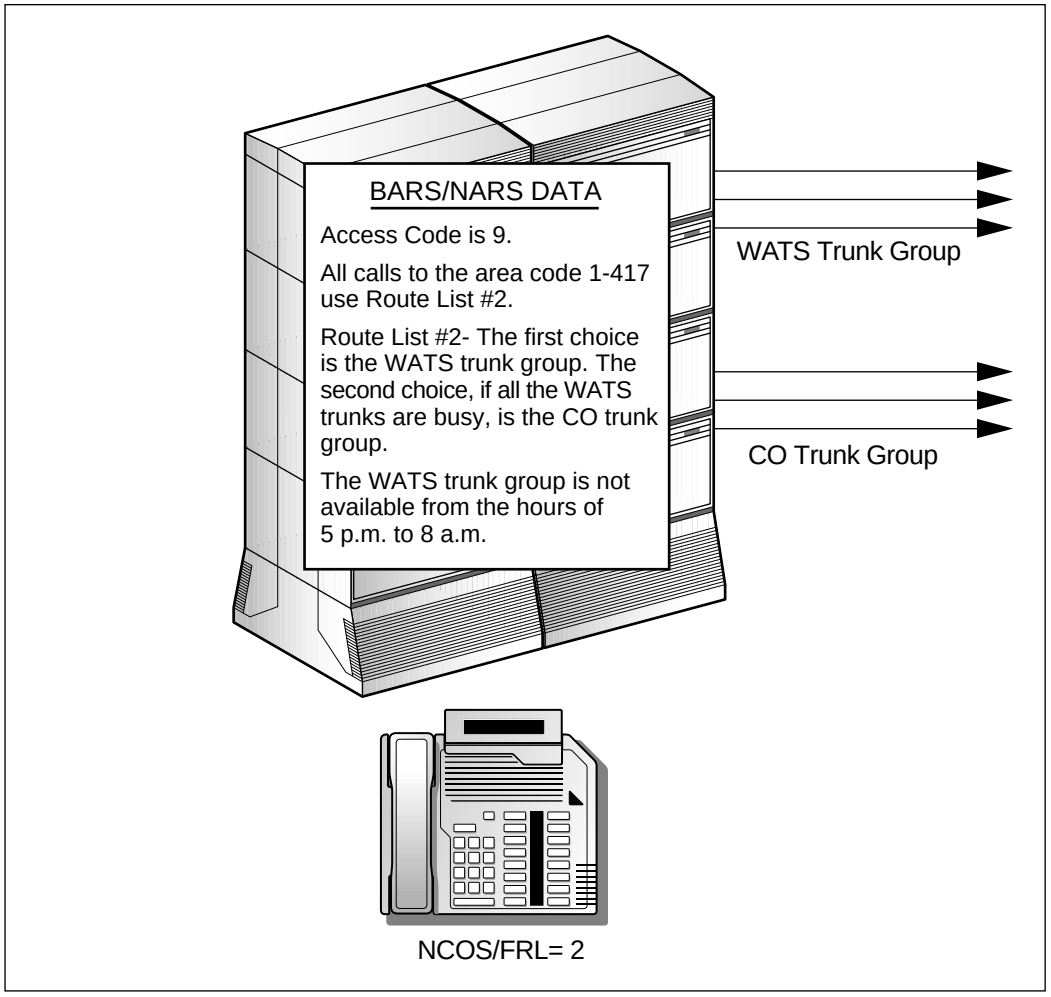
Time-of-day routing allows you to restrict access to certain destinations during specified time frames. For example, because the majority of fraudulent toll calls occur on holidays or after normal business hours, you can use this feature to turn off the route lists supporting calls to international locations or to the 809 area code after hours. Whether you can take this action depends on the needs of your user community.

How this feature works

The Time-of-Day Routing feature specifies the hours that users can access each entry in a route list. BARS/NARS provides for up to eight time-of-day schedules. With this feature you can specify the most cost-effective route alternatives based on the time of day, and restrict employees from calling locations they have no need to call for business purposes at certain hours.

Example

The following illustration shows how the Time-of-Day Routing feature works.


BARS/NARS DATA
Access Code is 9.
All calls to the area code 1-417 use Route List #2.
Route List #2- The first choice is the WATS trunk group. The second choice, if all the WATS trunks are busy, is the CO trunk group.
The WATS trunk group is not available from the hours of 5 p.m. to 8 a.m.
WATS Trunk Group
CO Trunk Group
NCOS/FRL= 2

G100457

In the example, the following occurs:

- The user dials 9-1-417-555-9090 at 6:00 p.m.
- 9 triggers the Meridian 1 software to use BARS/NARS data.
- The system checks the Translation Table.
- Calls to 417 use Route List Index 2.

Example (cont'd)

- The system searches Route List Index 2.
- The first choice, a WATS Route, is not available at 6:00 p.m.
- The second choice, CO Trunks, is available, and the call is sent out over the CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN TODS	LD 87 by ESN
Route List Index	LD 86—RLB TOD	LD 86 by RLB

Routing Control

Introduction

Again, because the majority of toll fraud and internal abuse occurs after normal business hours, or on weekends or holidays, you may want to program the system to automatically modify users' calling privileges during these times.

Description

The Routing Control feature lets you reduce or raise a user's network access capabilities if necessary.

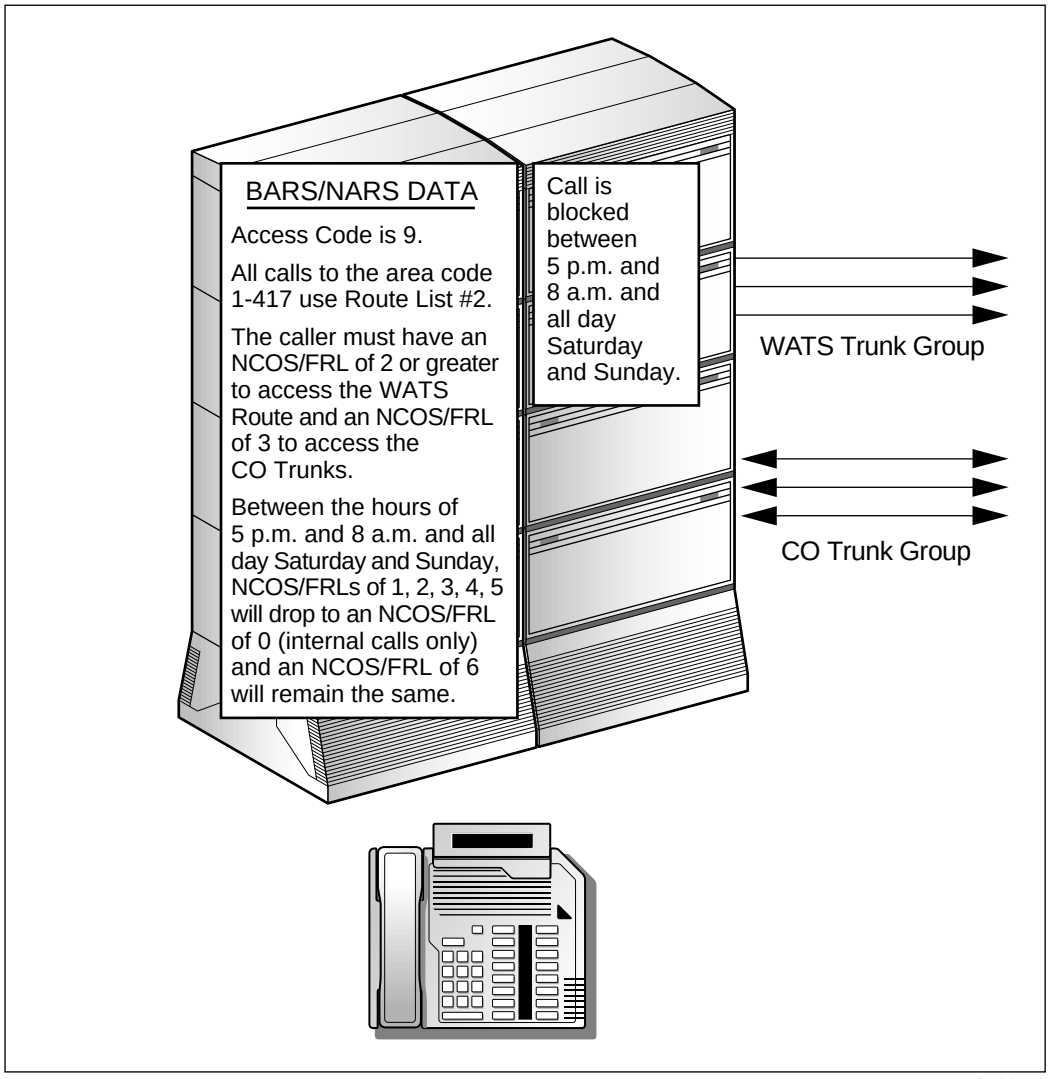
How Routing Control works

Each Network Class of Service (NCOS) is assigned an alternate NCOS when a special time-of-day schedule is in effect or during a specified day of the week. This feature enables you to change calling privileges automatically for a defined time frame each day or on weekends. You can also place a key on the attendant console that will manually activate routing control. With these features, you can implement controls on holidays and in response to critical situations.

Activating this feature prevents people from accessing unattended stations after hours to place unauthorized calls. However, authorization codes are not subject to the alternate NCOS assignments imposed through Routing Control. When users enter a valid authorization code, they are provided with the NCOS assigned to the authorization code for the duration of the call.

Example

The following illustration shows how the Routing Control feature works.


BARS/NARS DATA
Access Code is 9.
All calls to the area code 1-417 use Route List #2.
The caller must have an NCOS/FRL of 2 or greater to access the WATS Route and an NCOS/FRL of 3 to access the CO Trunks.
Between the hours of 5 p.m. and 8 a.m. and all day Saturday and Sunday, NCOS/FRLs of 1, 2, 3, 4, 5 will drop to an NCOS/FRL of 0 (internal calls only) and an NCOS/FRL of 6 will remain the same.
Call is blocked between 5 p.m. and 8 a.m. and all day Saturday and Sunday.
WATS Trunk Group
CO Trunk Group

G100458

In this example, the following takes place:

- The user dials 9-1-417-555-4436 at 9:00 p.m.
- 9 triggers the Meridian 1 to use BARS/NARS data.

Example (cont'd)

- Between 5:00 p.m. and 8:00 a.m., all users with an NCOS/FRL of 2 drop to an NCOS/FRL of 0.
- Meridian 1 checks the Translation Table for 1417 and sends the call to Route List Index 2.
- A user must have an NCOS/FRL of 2 to access the WATS routes (first choice) and an NCOS/FRL of 3 to access the CO trunk group (second choice).
- Because it is between 5:00 p.m. and 8:00 a.m., the user's NCOS/FRL is 0.
- This call is not eligible for any route in the Route List Index.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN, TODS 7, RTCL, NMAP ETOD	LD 87 ESN
Attendant	LD 12—KEY	LD 20 by TN
Network Control	LD 87—NCTL NCOS	LD 87 by NCOS
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by Speed Call List
DISA	LD 24—NCOS	LD 24 by DISA DN

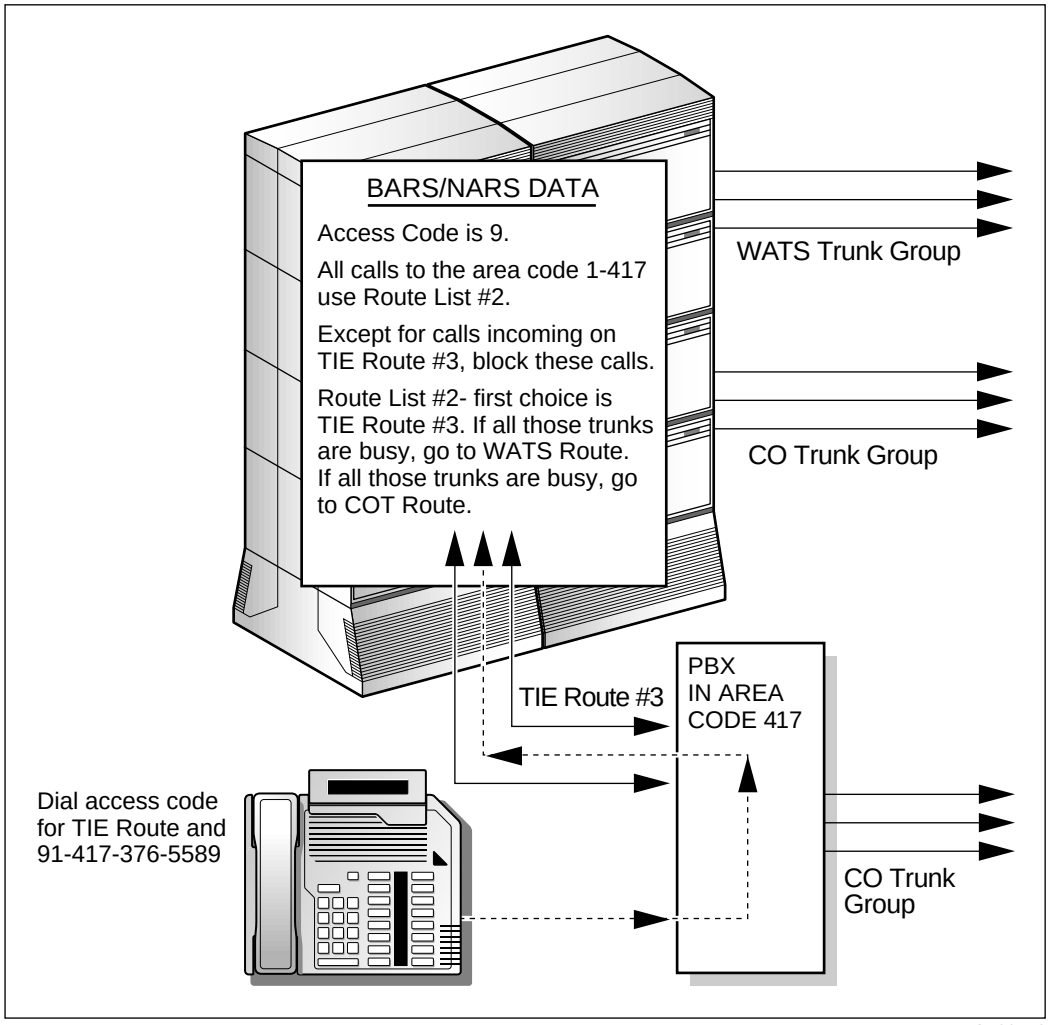
Incoming Trunk Group Exclusion

Description

You may want to control calls originating on various TIE routes. The Incoming Trunk Group Exclusion feature blocks BARS/NARS calls originating on TIE trunks from reaching destinations that employees do not need to reach for business purposes, and keeps users from attempting to circumvent the restrictions that are imposed at their home PBX. Each TIE route is associated with a table that defines the dialing sequences allowed for calls originated on that TIE route.

Example

The following figure illustrates how the Incoming Trunk Group (TIE) Exclusion feature works.


BARS/NARS DATA
Access Code is 9.
All calls to the area code 1-417 use Route List #2.
Except for calls incoming on TIE Route #3, block these calls.
Route List #2- first choice is TIE Route #3. If all those trunks are busy, go to WATS Route. If all those trunks are busy, go to COT Route.
WATS Trunk Group
CO Trunk Group
TIE Route #3
PBX
IN AREA
CODE 417
Dial access code for TIE Route and 91-417-376-5589
CO Trunk Group
G100459

In this figure, the following occurs:

- The user dials the access code for the TIE route and 9-1-417-555-5589.
- 9 triggers Meridian 1 to use BARS/NARS data.
- BARS/NARS checks the Translation Table for the 417 area code and finds it restricted for calls from TIE Route 3.

Example (cont'd)

- Meridian 1 validates that the call is incoming on TIE Route 3.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Incoming Trunk Group Exclusion feature.

For	Implement using	Print using
ESN	LD 87—FEAT=ESN MXSD, MXIX	LD 87 FEAT=ESN
Incoming Trunk Group Exclusion	LD 86—FEAT=ITGE all prompts	LD 86 FEAT=ITGE by Incoming Trunk Group Exclusion Index
Network Translation	LD 90—FEAT=NET ITED, ITEI	LD 90 FEAT=NET by NPA or NXX or SPN

Section F: Controlling access to PBX administration programs

In this section

Overview	7-74
Password control	7-75
Limited access to overlays	7-77
Limited access password—user name	7-78
Single Terminal Access	7-79
Multi-user login	7-80
Input/Output port recovery	7-81
History file	7-82

Overview

Introduction

You can use the following to control access to PBX administration programs:

- Password control
  - Level 1 password
  - Level 2 password

  For more information, see “Password control” on page 7-75.
- Limited access to overlays

  For more information, see “Limited access to overlays” on page 7-77.
- Limited access password—user name

  For more information, see “Limited access password—user name” on page 7-78.
- Single Terminal Access (STA)

  For more information, see “Single Terminal Access” on page 7-79.
- Multi-user login

  For more information, see “Multi-user login” on page 7-80.
- Input/Output port recovery

  For more information, see “Input/Output port recovery” on page 7-81.
- History file

  For more information, see “History file” on page 7-82.

Password control

Introduction

Hackers have been known to access a system to obtain printouts of valid authorization codes, reassign control characteristics, defeat security measures in place, or degrade system performance. By controlling system passwords, you can minimize unauthorized access to the system. You can define a number of passwords that administrators can use to access the system for the purpose of the database.

Two types of passwords

As of X11 Release 16, two types of passwords allow access to all aspects of the database and maintenance programs:

- Level 1 password
- Level 2 password

Level 1 password

You can use the Level 1 password to log on to the switch. Upon entering the valid password, you can change virtually all aspects of the database with the exception of changing the Level 1 and 2 passwords and, if defined, the secure data password associated with assigning authorization codes and DISA parameters.

Implementing and auditing the Level 1 password

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 1 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Level 2 password

The Level 2 password provides all the capabilities of the Level 1 password, and also allows you to change the Level 1 and Level 2 passwords as well as the secure data password.

Implementing and auditing the Level 2 password

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 2 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Limited access to overlays

Description

The Limited Access to Overlays (LAPW) feature introduced in X11 Release 16 provides a greater degree of control of password assignment and overlay access. In addition, it expands tracking of switch access.

This feature provides additional security by allowing you to define up to 100 LAPW passwords per system. The LAPW password may be 4 to 16 alphanumeric characters in both uppercase and lowercase. A maximum of four characters are allowed in either Password 1 or Password 2.

How LAPW works

You can define access to specific overlays for each password and specify a "Print-only" capability. You can also configure an audit trail to record the date, time, and password used, and the overlay programs accessed.

The system monitors failed logon attempts, compares the number with a predefined threshold, and locks the entry port if the threshold is exceeded. The Meridian 1 reports lock-out conditions on all TTYs and provides a special report to the next administrator who logs on.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access to Overlays feature.

For	Implement using	Print using
Configuration	LD 17—LAPW, PWNN, OVLY, CUST, TEN, OPT, LPWED, NLPW, FLTH, LOCK, AUDT, SIZE, INIT	LD 22 by CFN or LAPW from Release 19 and up

Limited access password—user name

Introduction

In addition to Level 1 and Level 2 passwords and the 100 limited access passwords, Release 19 can also require users to enter a user name with up to eight alphanumeric characters. Only the Level 2 password can configure user names, and change and print all passwords.

LAPW users may change their own passwords but not their user names.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access Password feature.

For	Implement using	Print using
CFN	LD 17—LNAME_OPTION, LOGIN_NAME	LD 22 TYPE CFN, AUDT from Release 19 and up

Single Terminal Access

Description

The Single Terminal Access feature (STA) introduced in Release 19 provides an integrated solution to reduce the number of physical devices needed to administer and maintain a Meridian 1 system and its associated subsystems.

How STA works

A mechanism for ensuring the terminal of the original session when the user intends to switch to another system is provided in the STA application through a user-determined logout sequence. Specified in the database with each STA port, this sequence will automatically be sent to the destination system by the application to prevent users from leaving a session open in the background without logging out. If the logout sequence is not programmed or programmed incorrectly, the user could leave a program open in the background and subject to unauthorized access.

The STA master terminal will use the configured logout sequence to automatically exit from the active and existing background sessions when the modem connection for the terminal experiences carrier dropout.

A password is required before the user can new or change the configuration of STA ports. This process is designed to protect the STA port from unauthorized alteration.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Single Terminal Access feature.

For	Implement using	Print using
Configuration record	LD 17—ADAN, TTY, CTYP, GRP, DNUM, PORT, DES, BPS, PRTY, STOP, BITL, PARM, FUNC, USER, MPRT, APRT	LD 22 by CFN, or ADAN from Release 19 and up

Multi-user login

Description

Multi-user login allows up to three users to simultaneously log in to a Meridian 1 PBX to load and execute overlays. A fourth overlay running in the background or at midnight is also allowed.

The feature is activated and deactivated in Overlay 17.

Release 19 support

Release 19 supports only Set Administration (Overlays 10 and 11), associated print loads (Overlays 20, 21, and 22), Maintenance, Midnight Routines, Background Routines, or Attendant Administration.

Forced logoff

Additionally, a user can force the logoff from a specific terminal when logged in to the Level Password or an appropriate Limited Access Password.

Monitoring input/ output

The monitor command allows a logged in user to monitor the input/output of a different specified terminal either locally or remotely; this feature is assigned on a per password level or to the Level 2 password.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Multi-user Login feature.

For	Implement using	Print using
CFN	LD 17—PWD2, LAPW, TLOG, SIZE, MULTI-USER, OPT	LD 22 PRT by CFN or LAPW from Release 19 and up

Input/Output port recovery

Introduction

Ports defined as TTY and PRT are controlled by two counters monitoring invalid characters. Ports disabled due to garbage characters or interference can be automatically enabled after a four-minute timer has expired.

Disabled ports can be enabled a maximum of three times in 30 minutes. The fourth time a port is disabled in a 30-minute period requires manual enabling. Messages print at the TTY each time the port disables and reenables.

Implementing and auditing the feature

The documentation is built into the base software.

No alteration is possible.

History file

Description

You may want to track certain system messages or activity and print that information at will. The History file stores system messages in memory. You can access the stored information through a system TTY or from a remote location, and you can print its contents.

How the History file works

You can specify the types of information that you want to store in the History file including maintenance messages (MTC), service change activity (SCH), customer service change activity (CSC), traffic outputs (TRF), and software error messages (ERR and BUG). By storing SCH activity and TRF output messages, you can store records of unauthorized access to the switch and retrieve information associated with calling patterns.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the History file feature.

For	Implement using	Print using
LD1F Configuration	LD 17—IOTB, HIST, ADAN, USER	LD 22 CFN or ADAN from Release 19 and up

Release 19 enhancements

With Release 19, you may selectively view the History file using the command VHST. Commands allow you to search forward, repeat the last forward or backward search, and perform other various navigational movements within the file.

The History file may also have three categories of files: Log files (see “Multi-user login” on page 7-80), System History file, and Traffic files. Traffic files have two categories: system (scheduled) or user-generated reports. There is one traffic file per system.

These enhancements are included in the base software package.

Section G: Controlling Direct Inward System Access

In this section

Overview	7-84
DISA and security codes	7-85
DISA and Class of Service	7-86
DISA and authorization codes	7-87

Overview

Description: DISA

Direct Inward System Access (DISA) provides a convenient means by which employees, when they are offsite, can place calls to internal extensions, and to private and public network locations by accessing your company's switching system.

How DISA is abused

The type of unauthorized access associated with this feature begins when perpetrators find the telephone number associated with DISA. In most DISA intrusion cases, hackers use PC-based programs to obtain valid DISA DNs, and security and authorization codes. Once a PC program finds a valid DISA telephone number, the PC inputs codes, redials the telephone number repeatedly, and stores the valid codes. Hackers then sell the numbers and codes they obtain illegally to third parties who then use this information for their own "business purposes."

In this section

In this section, you will learn how to effectively manage and monitor the Meridian 1 DISA feature.

DISA and security codes

Introduction

The first level of restricting DISA access is the security code.

How security codes work

If you program your system to require a security code, when the Meridian 1 answers a DISA call, callers must enter the security code assigned to the DISA DN before they can gain access to the system. This security code can be from one to eight digits long.

Remember, the longer the code, the harder it is for a hacker to crack.

DISA and Class of Service

Introduction

The second level of restriction is the class of service assigned to the DISA DN. Each DISA DN has its own Class of Service (COS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS).

How Class of Service works

When the Meridian 1 answers, if you do not require callers to enter authorization codes, then they automatically receive the DISA DN's calling privileges and class of service. You should consider making these controls as restrictive as possible (internal calls only, for example) and force users to enter an authorization code to access trunking facilities.

In addition, if the Meridian 1 records authorization codes in Call Detail Recording (CDR), you can track calls made through DISA and bill them back to users.

Implementing this feature

To implement this feature, see "Class of Service" on page 7-13.

DISA and authorization codes

Introduction

For a third level of security, you can require callers to enter an authorization code before they gain access to system facilities. You can assign authorization codes that are from 1 to 14 digits long. By assigning 14-digit authorization codes, you ensure that the hacker's PC-based code-cracking program has to try more combinations to obtain valid codes.

You can also configure Call Detail Recording to output the authorization codes used for call placement. In reviewing these reports, you should investigate any surge in activity for a given authorization code.

Assigning and changing codes

For further security, you should change authorization codes often and assign one code per person. If you cannot change authorization codes often because you have assigned a large number of codes and communicating the change would be difficult, then consider changing the DISA security code often.

Removal of codes

You should remove the authorization codes of terminated employees immediately. Establish a procedure with Human Resources or your Personnel department to advise you when employees leave the company.

Section H: Restriction/Permission lists

In this section

Overview	7-90
What are restriction/permission lists and codes?	7-91
Defaults	7-93
Understanding how restriction/permission codes work	7-94
Recommendations for using the first four restriction/ permission lists	7-97
Defining and applying restriction/permission lists	7-99

Overview

Introduction

In today's telecommunications environment, the same features that provide you with flexibility can also be the source of unauthorized use and abuse.

Meridian Mail features

Features such as remote notification, external call sender, call answering/express messaging thru-dial, and AMIS networking can dial numbers external to your telephone switch. This means that they can be used by users or external callers to place unauthorized long-distance calls at your organization's expense.

Restriction/ permission lists

The primary weapon in your outcalling security arsenal are the restriction/permission lists. These lists are your first line of defense.

What are restriction/permission lists and codes?

Introduction

Restriction/permission lists are an important part of preventing users and callers from abusing your Meridian Mail system.

Definition: restriction/permission list

A restriction/permission list is a group (or set) of restriction codes and permission dialing codes that can be applied to Meridian Mail features or services that are capable of placing outcalls.

Up to 80 lists can be created, but each list must have a unique name. Each list can have up to 30 restriction codes and up to 30 permission codes. Once a list is defined, it can be applied to a number of Meridian Mail features.

Definition: restriction code

A restriction code is a dialing code that Meridian Mail is not permitted to dial. When Meridian Mail is passed a number that begins with a restricted code, the call is blocked.

Restriction codes can be up to 20 digits in length.

Example 1
Your local dialing prefix is 9, your long distance dialing prefix is 91, and your international dialing prefix is 9011. You want to restrict all off-switch dialing. The restriction code is 9.

Example 2
Your long distance dialing prefix is 91 and you want to restrict calls to the 801 area code. The resulting restriction code is 91801.

Definition: permission code

A permission code is a dialing code that Meridian Mail is permitted to dial. These are usually exceptions to the restriction "rules."

Permission codes can be up to 20 digits in length.

Example of a restriction/permission list

In this example, 91 is the long distance dialing prefix and 9011 is the international dialing prefix. All internal extensions begin with 7 and 8.

List Name: Local

Restriction codes: 1 2 3 4 5 6 91 9011

Permission codes: 91617 911

This list restricts all international and long-distance calls, except those to 911 and to the 617 area code. In addition to the permitted codes, it allows on-switch calls to internal extensions beginning with 7 or 8, and local calls beginning with 9.

Defaults

Introduction

The defaults for new installations and conversions are described here. The default values when you first view a restriction/permission list are also described.

Defaults for new installations

For newly installed Meridian Mail Release 12 systems, all restriction/permission lists are fully restricted. The first four lists are named On_Switch, Local, Long_distance_1, and Long_Distance_2, and the remaining 76 lists are named RPList5 to RPList80 respectively.

> **ATTENTION**
>
> You must modify restriction/permission lists after installation. If you do not, many Meridian Mail features that place outcalls will not work.

Defaults for converted systems

If you have converted to Release 12, the four existing restriction/permission lists remain as they were in the previous release. The new lists are named RPList5 to RPList80 and are fully restricted.

Note: Even though the codes remain the same, you must apply restrictions to any new Release 12 features you implement.

Default list entries

If you have not modified a restriction/permission list, it will be defined as follows the first time you view it:

Restriction codes: 0 1 2 3 4 5 6 7 8 9

Permission codes: (none)

Understanding how restriction/permission codes work

Introduction

The restriction codes in a restriction/permission list specify the general dialing rule. Permission codes are used to indicate any exceptions to the more general rules described by the restriction codes.

Levels of security

It is up to your organization to decide how to configure the restriction/permission lists. They are typically configured to provide various levels of security, from permitting only on-switch dialing (most secure) to allowing all long-distance dialing (least secure).

Examples

The following table contains examples of restriction/permission codes and how Meridian Mail interprets them.

In these examples, 9 is the dialing code for local calls, and 91 is the dialing code for long distance calls.

Restriction code(s)	Permission code(s)	Result
91	91416, 9911	Most long distance calls are restricted, except for 911 calls and numbers in the 416 area code.
1, 2, 5, 6, 7, 8, 9	none	All local and long distance calls are restricted. Internal extensions beginning with 3 or 4 are allowed.
91900	9	1-900 numbers are restricted, but local calls and all other long distance calls are permitted.

Rule

Numbers beginning with a permission code that is shorter than a restriction code and that matches a subset of the restriction code are allowed. They are not restricted.

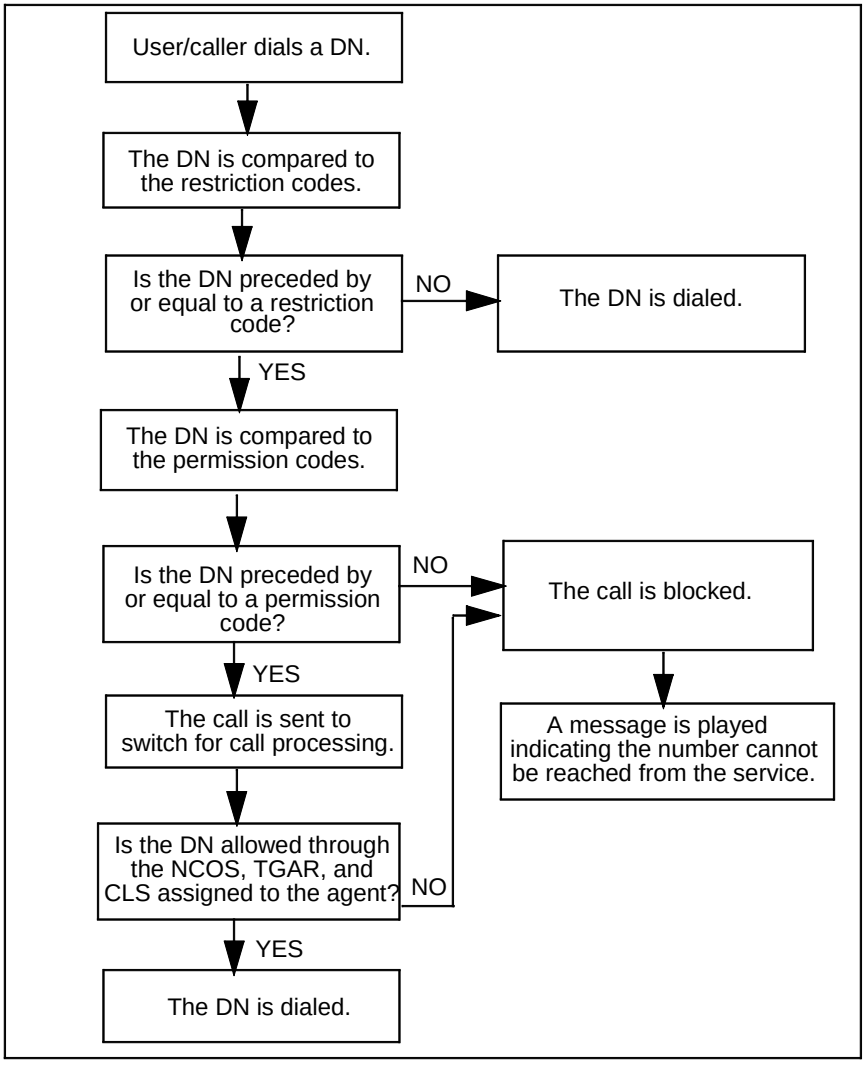
Rule (cont'd)

Example

91900 is a restriction code. 9 is a permission code. Calls beginning with 9 (local calls) or 91 (long distance) are permitted as long as they are not to 91900.

How restriction/ permission codes are processed

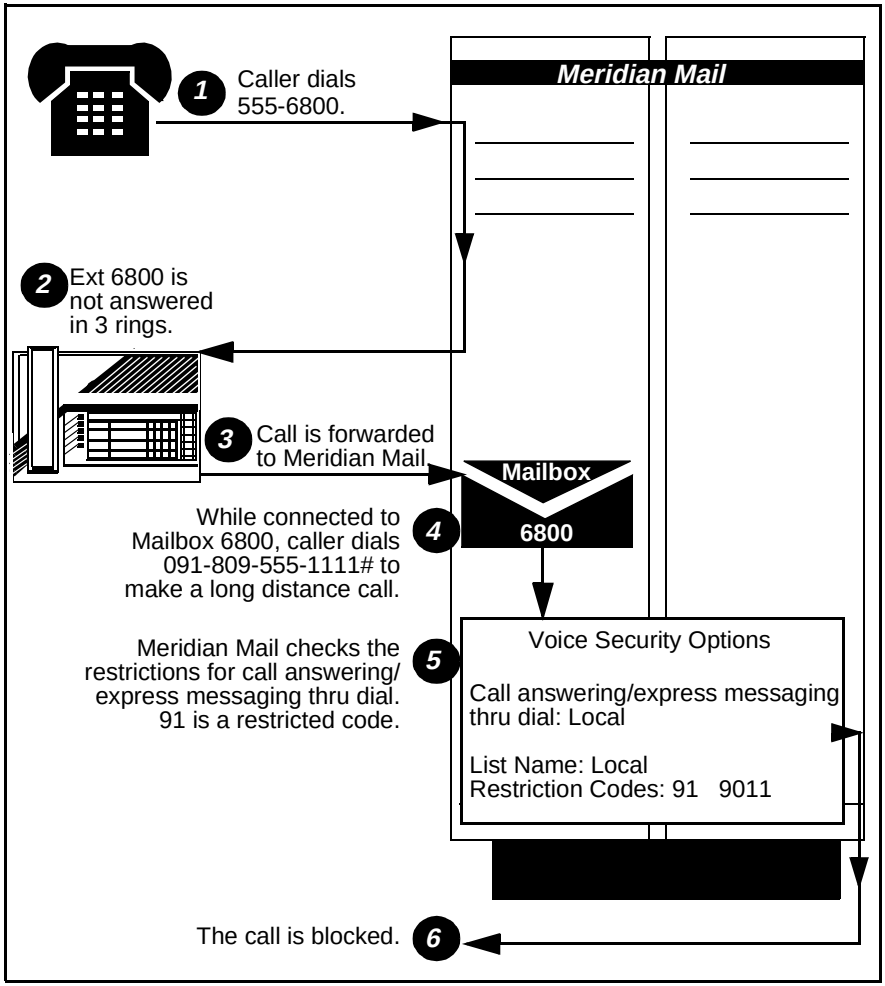
The following flowchart shows how Meridian Mail and the Meridian 1 process restriction and permission codes when a DN is dialed.


User/caller dials a DN.
The DN is compared to the restriction codes.
Is the DN preceded by or equal to a restriction code?
NO
The DN is dialed.
YES
The DN is compared to the permission codes.
Is the DN preceded by or equal to a permission code?
NO
The call is blocked.
YES
The call is sent to switch for call processing.
A message is played indicating the number cannot be reached from the service.
Is the DN allowed through the NCOS, TGAR, and CLS assigned to the agent?
NO
YES
The DN is dialed.

Example: Call answering thru-dial

Call answering/express messaging thru-dial allows callers to transfer to another internal extension or valid telephone number once Meridian Mail answers. If the proper restrictions are not placed on this feature, callers will be able to place calls at your organization's expense.

The following illustration shows how restriction/permission codes work in the case of call answering thru-dial.


Meridian Mail
1
Caller dials 555-6800.
2
Ext 6800 is not answered in 3 rings.
3
Call is forwarded to Meridian Mail.
Mailbox
6800
4
While connected to Mailbox 6800, caller dials 091-809-555-1111# to make a long distance call.
5
Meridian Mail checks the restrictions for call answering/ express messaging thru dial. 91 is a restricted code.
Voice Security Options
Call answering/express messaging thru dial: Local
List Name: Local
Restriction Codes: 91 9011
6
The call is blocked.

Recommendations for using the first four restriction/ permission lists

Introduction

The first four restriction/permission lists are named as follows:

- On_Switch
- Local
- Long_Distance_1
- Long_Distance_2

These names can be changed.

Recommendations

Nortel recommends that you use the default restriction/ permission lists as follows.

Note: You are responsible for developing a policy for restricting outcalling that is suitable to your organization's needs.

List name	List function	Restriction codes	Permission codes
On-switch	Permits calls to on-switch extensions only. Restricts all local, long distance, and international calls.	• local dialing prefix • long distance dialing prefix • international dialing prefix	optional (as required)
Local	Permits all on-switch and local calls. Restricts all long distance and international calls.	• long distance dialing prefix • international dialing prefix	optional (as required)

List name	List function	Restriction codes	Permission codes
Long Distance 1	Permits all on-switch calls, local calls, and long distance calls to certain area codes only. Restricts all international calls and long distance calls (in general).	• long distance dialing prefix • international dialing prefix	• specific long distance area codes
Long Distance 2	Permits all on-switch, local, and long distance calls. Restricts all international calls. or Permits all on-switch calls, local calls, and long distance calls to certain area codes only. (Similar in function to Long Distance 1, but permits different area codes.) Restricts all international calls and long distance calls (in general).	• international dialing prefix or • long distance dialing prefix • international dialing prefix • specific area codes	• none or • specific area codes

Defining and applying restriction/permission lists

Introduction

Restriction/permission lists can only be defined through the Restriction/Permission Lists screen. They are, however, applied to specific Meridian Mail features or services through other screens.

Defining restriction/ permission lists

To define restriction/permission lists, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Restriction/Permission Lists. **Result:** The Restriction/Permission Lists screen appears.
3	Position the cursor beside the List number you want to view or modify.
4	Press the [SpaceBar] to highlight the list.
5	Press the [View/Modify] softkey. **Result:** The View/Modify Restriction/Permission List screen appears.
6	Do you want to modify or view the codes in the list?

IF you want to	THEN
modify the list	go to step 7.
view the file	use the cursor keys to scroll through the screen and then go to step 10.

7 Do you want to change the list name?

IF	THEN
yes	press [Backspace] to delete the current name. Enter the new list name.
no	go to step 8.

Step	Action
8	Do you want to change the restriction codes?

IF	THEN
yes	delete the existing code (if not appropriate) and enter a new code. Press <Return> or <Tab> to move to the next field.
no	go to step 9.

Step	Action
9	Do you want to change the permission codes?

IF	THEN
yes	enter the new code. Press <Return> or <Tab> to move to the next field.
no	go to step 10.

Step	Action
10	Do you want to save your changes?

IF	THEN
yes	press [Save].
no	press [Cancel].

Result: The Restriction/Permission Lists screen appears.

Applying restriction/permission lists

The following table identifies which Meridian Mail screens are used to apply restriction/permission lists to Meridian Mail features or services.

To apply restrictions/permissions to the following feature	Use the following screen
Call Answering/Express Messaging Thru-Dial	Voice Security Options
Fax Information service	Session Profile (accessed from the VSDN table; necessary only if Fax on Demand is installed). For more information, refer to the *Fax on Demand Application Guide* (NTP 555-7001-327).
Fax Item Maintenance service	
Voice Menus (that activate fax service)	
Time-of-Day Controllers (that activate fax service)	
Extension dialing (mailbox thru-dial)	Add (or View/Modify) Class of Service
Custom Operator revert	
Remote Notification	
Delivery to Non-User	
External Call Sender	
AMIS Networking	
Thru-Dial service	Add (or View/Modify) Thru-Dial Definition

Section I: Controlling access to Meridian Mail services and features

In this section

Overview	7-104
Custom Revert	7-106
Thru-Dial	7-109
Call Answering or Express Messaging	7-110
Extension dialing (mailbox thru-dial)	7-112
Fax on Demand	7-115
Remote Notification	7-116
Delivery to Non-User	7-118
External Call sender	7-120
AMIS Networking	7-121

Overview

Introduction

Meridian Mail is a voice mail system that is integrated into the Meridian 1 PBX. One of the most feature-rich voice messaging products on the market, the system provides flexible features like Voice Menus which allow callers to choose from lists of services, and Remote Notification which notifies off-site system users that they have messages waiting.

Restriction/ permission lists

You can minimize the risk of toll fraud and system abuse by using the restriction/permission features to control access to your Meridian Mail system and switch. If you fail to put the proper safeguards in place, callers answered by your voice mail system can place toll calls.

Restriction permission lists are applied to features that are capable of dialing outside your switch and are, therefore, a potential source of unauthorized system use and abuse.

Features to which restriction/permission lists can be applied

Restriction/permission lists can be applied to the following features.

Feature	Description
Custom (operator) revert	Users can define their own Custom Revert DN. Assign a list to this feature to restrict the DNs that users can specify.
Thru-dial services	Once connected to a thru-dial service, callers can thru-dial to external numbers if restrictions are not in place. Assign a list to all thru-dialers to restrict the numbers to which callers can thru-dial.
Call answering/ Express messaging Thru-dial	Callers can transfer to other numbers during call answering and express messaging sessions. Assign a list to this feature to restrict the numbers to which callers are allowed to transfer themselves.
Extension dialing (mailbox thru-dial)	Users can thru-dial to other numbers while they are logged on to their mailbox. Assign a list to this feature to restrict the numbers to which they are allowed to thru-dial.

Feature	Description
Fax information service	Callers can request faxes using this service. Assign a list to this feature to restrict the numbers to which faxes are sent.
Fax item maintenance	This service is used to send verification faxes to designated fax phones. Assign a list to this feature to restrict the numbers to which verification faxes can be sent.
Remote notification	Users can set up their own remote notification schedules which specify the remote device (phone, pager) to which notification of new messages should be sent. Assign a list to this feature to restrict the numbers at which users can be remotely notified.
Delivery to non-users	Users can send voice messages to people who do not have mailboxes. Assign a list to this feature to restrict the non-user numbers to which users can send voice messages.
Call sender	Users can return a call with a single telephone set command (9). Assign a list to restrict the numbers they can call back with external call sender.
AMIS Networking	Users can send voice messages to other voice mail systems. Assign a list to this feature to restrict the voice mail systems to which users can send messages.

Custom Revert

Introduction

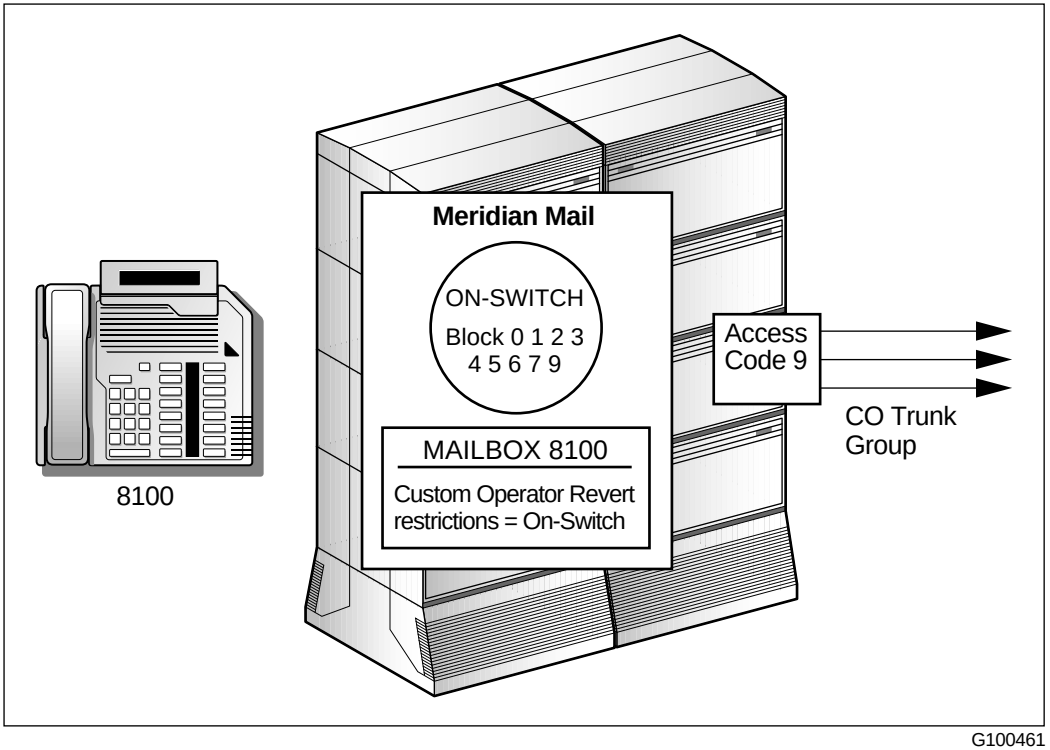
Once Meridian Mail answers, callers may dial zero (0) anytime during the personal greeting or during the record cycle, and transfer to a predefined extension, usually a receptionist or secretary. This extension is the Revert DN.

Description

Each mailbox user can define his or her own Custom Revert DN through the telephone set. To prevent users from (unknowingly) abusing the system, you should assign restriction/permission lists to the revert feature.

Example

The following illustration shows how the Custom Operator Revert feature works.



G100461

Example (cont'd)

In this example, the following takes place:

- The user logs in to Meridian Mail.
- The user activates the Custom Operator Revert feature and attempts to define the operator revert as 9-555-0000.
- Meridian Mail checks the Custom Operator Revert restrictions.
- The On-Switch Table blocks the code 9, and the function is disallowed.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 7-99.

Assigning a restriction/permission list

To assign a restriction/permission list to the Custom Revert feature, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action
4	Position the cursor beside the Custom Revert Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Custom Revert feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Thru-Dial

Introduction

All Thru-Dial services you create using the Voice Menus feature must be adequately protected with an appropriate restriction/permission list.

Defining a restriction/ permission list

To define a restriction/permission list, see “Defining and applying restriction/permission lists” on page 7-99.

Assigning a restriction/permission list

To assign a restriction/permission list to the Thru-Dial service, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Voice Administration from the Main Menu.
3	Select Voice Services Administration from the Voice Administration menu.
4	Select Thru-Dial Definitions.
5	Position the cursor beside the definition, and press the [SpaceBar].
6	Press [View/Modify].
7	Position the cursor beside the Restriction/Permission List field.
8	Enter the number of the restriction/permission list you want to assign to the feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
9	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

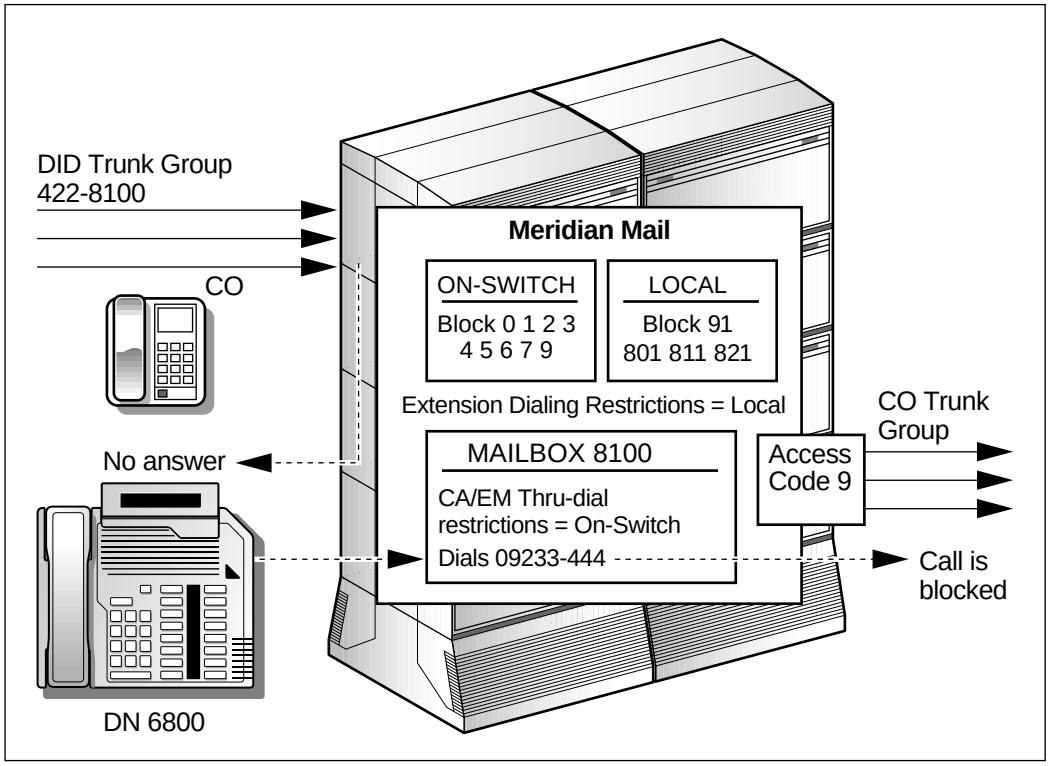
Call Answering or Express Messaging

Description

During a call answering or express messaging session, an external caller could potentially use thru-dial capabilities to place unauthorized calls which would be billed to the system. To use Thru-Dial, a caller must press 0 followed by a dialable DN. (If the caller waits more than two seconds after entering 0, he or she will be connected to an attendant instead.)

Example

The following illustration shows how the extension dialing feature works during a Call Answering/Express Messaging session.



G100462

Example (cont'd)

In this example, the following takes place:

- The caller dials 555-8100. No answer is encountered at extension 8100.
- The caller is forwarded to Meridian Mail.
- Once answered, the caller dials 09233-44.
- Meridian Mail checks the Call Answering/Express Messaging Thru-dial restrictions.
- 9 is not allowed so the call is blocked. If the caller had logged in to Meridian Mail, the call would have been allowed.

Restricting thru-dial capabilities

To prevent callers and users from abusing thru-dial capabilities during call answering or express messaging sessions, make sure an appropriate restriction/permission list is applied to call answering or express messaging thru-dial in the Voice Security Options screen.

To restrict thru-dial capabilities for call answering or express messaging sessions, use the following procedure.

Step	Action
1	Select Voice Administration from the Main Menu.
2	Select Voice Security Options.
3	Move the cursor to the Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number field.
4	Enter the number of the restriction/permission list you want to apply to call answering and express messaging thru-dial. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is moved off the field.
5	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Extension dialing (mailbox thru-dial)

Description

Another standard feature available with Meridian Mail is extension dialing, or Thru-dial for mailboxes. The extension dialing feature allows callers to transfer to another extension number or valid telephone number once they log in to Meridian Mail. Callers can dial zero (0) followed by an extension number, or valid access code, telephone number, and the pound sign (#).

This feature only applies to MMUI systems.

Controls you can exercise

Meridian Mail is shipped with the mailbox Thru-dial feature turned on. You can control access and use of Thru-dial in two ways:

- within the Meridian Mail system
- within the Meridian 1 system through the virtual agent

Controlling access within Meridian Mail

This method allows you to define and apply the restrictions codes that best fit the needs of your user community and the security requirements of your organization.

This method involves

- defining restriction permission lists

  (see “Defining and applying restriction/permission lists” on page 7-99)
- applying restriction/permission lists to features

Note: See “Applying a restriction/permission list” on page 7-113. These codes affect *all* mailbox Thru-dial functions that use the same Class of Service.

Applying a restriction/ permission list

To apply a restriction/permission list, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Position the cursor beside the Extension Dialing Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Extension dialing feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

Controlling access within the switch

To control access of the Thru-dial feature within the Meridian 1 system, use the following procedure. This method allows you to restrict the Thru-dial feature through the virtual agent.

Note 1: To restrict all access to the outside world through Thru-dial, be sure to restrict both your Least Cost Routing access code and your direct access code to each trunk group in the Meridian 1.

Note 2: Be sure to block access to your Special Prefix (SPRE) code as well.

Step	Action
1	Assign the appropriate Network Class of Service (NCOS). For more information, see “Network Class of Service—Facility Restriction Level” on page 7-55.
2	Assign the appropriate Trunk Group Access Restrictions (TGAR). For more information, see “Trunk Group Access Restrictions” on page 7-11.
3	Assign the appropriate Class of Service (COS). For more information, see “Class of Service” on page 7-13.

The restrictions you impose through the virtual agent apply to Thru-dial functions accessed both through the voice menus feature and at the mailbox level.

Fax on Demand

Description

If Fax on Demand is installed, you will need to determine the restrictions that need to be applied to external callers who request that faxes be delivered using callback delivery. In other words, with callback delivery, callers are asked to specify the number to which a fax should be delivered. You will have to decide if you want faxes to be delivered to all numbers, only local numbers, all long distance numbers, only certain area codes, and so on.

Note: This topic is only applicable to systems that have Fax on Demand installed.

Restricting thru-dial for Fax on Demand

When adding the VSDN of the service through which the fax item will be made accessible, you must specify a session profile. In this session profile, you choose the fax delivery method. If it is set to either Call Back or Caller Choice, you will have to specify a restriction/permission list (also in the session profile).

Refer to the *Fax on Demand Application Guide* (NTP 555-7001-327) for information on securing the callback options.

Remote Notification

Description

Remote Notification allows a user to be notified at a remote telephone or pages when a new message arrives in his or her mailbox. Users can define their own remote notification schedules and target DNs from their telephone sets.

Note: This topic is only applicable to systems that have the Outcalling feature installed.

Restricting target DNs

To restrict the target DNs to which users try to send remote notifications, you must assign a restriction/permission list to the Remote Notification feature in the classes of service you set up.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 7-99.

Applying a restriction/ permission list

To apply a restriction/permission list to the Remote Notification, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action
4	Do you want to enable Remote Notification capabilities for this class of service?

IF	THEN go to
yes	step 5.
no	step 9.

Step	Action
5	Set the Remote Notification Capability field to Yes. **Result:** The following four fields will appear: • Remote Notification Restriction/Permission List • Remote Notification Keypad Interface • Remote Notification Retry Limits and Frequency • RN Business Days
6	Enter the number of the restriction/permission list you want to assign to the feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
7	Do you want your users in this class of service to be able to use their keypad interface to change the remote notification DN? **Note:** The Keypad Interface field applies only to MMUI systems.

IF	THEN set the Keypad Interface field to
yes	yes.
no	no.

Step	Action
8	Enter the retry limits and frequencies for the following: • Busy • No Answer • Answered
9	Select the business days on which remote notification will (not) be available.
10	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Delivery to Non-User

Description

Delivery to Non-User (DNU) allows a Meridian Mail user to compose and send a voice message to someone who is not a Meridian Mail user. To restrict the numbers to which users are allowed to send voice messages, assign an appropriate restriction/permission list to the Delivery to Non-User feature in the classes of service you set up.

Note: This topic is only applicable to systems that have the Outcalling feature installed.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 7-99.

Applying a restriction/ permission list

To apply a restriction/permission list to the Delivery to Non-user feature, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Do you want to enable Delivery to Non-User capabilities for this class of service?

IF	THEN go to
yes	step 5.
no	step 9.

Step Action

5 Set the Delivery to Non-User Capability field to Yes.

Result: The following three fields appear:

- Delivery to Non-User Restriction/Permission List
- Send Messages via DNU if Mailbox Not Found
- DNU DTMF Confirmation Required

6 Enter the number of the restriction/permission list you want to assign to the feature.

Note: The name of the corresponding restriction/permission list does not appear until the cursor is off the field.

7 Do you want to send messages if the mailbox is not found?

IF	THEN set the Send Messages via DNU if Mailbox Not Found field to
yes	Yes.
no	No.

8 Do you require a DTMF confirmation?

IF	THEN set the DNU DTMF Confirmation Required field to
yes	Yes.
no	No.

9 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

External Call sender

Description

This feature allows a Meridian Mail user to immediately call back someone who has left a message and who is external to the switch, by pressing 9 after listening to the message. (This only applies to messages that have been left during call answering sessions, and composed voice messages.)

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 7-99.

Applying a restriction/ permission list

To apply a restriction/permission list to External Call Sender, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Position the cursor beside the External Call Sender Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Call Sender feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

AMIS Networking

Description

When a user composes a voice message and tries to send it to an AMIS site (that is not defined as a virtual node), Meridian Mail checks the restriction/permission list that is assigned to AMIS networking to see if it is restricted. The restriction/permission list is assigned to AMIS networking in classes of service.

Note: This topic is only applicable to systems that have the AMIS Networking feature installed.

Virtual Node AMIS

In the case of Virtual Node AMIS, where the local site also has Meridian Networking, these restrictions do not apply to remote AMIS sites that are defined as virtual nodes in the local network database.

For more information on Virtual Node AMIS, refer to the *Virtual Node AMIS Installation and Administration Guide* (NTP 555-7001-245).

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 7-99.

Applying a restriction/ permission list

To apply a restriction/permission list to AMIS Networking, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action
4	Do you want mailbox users assigned to this class of service to be able to receive AMIS Open Network Messages?

IF	THEN set the Receive AMIS Open Network Messages field to
yes	Yes.
no	No.

Step	Action
5	Do you want mailbox users assigned to this class of service to be able to compose and send AMIS Open Network Messages?

IF	THEN set the Compose/Send AMIS Open Network Messages field to
yes	Yes.
no	No.

Result: The following field appears when the field is set to Yes:

- AMIS Open Network Restriction/Permission List

Step	Action
6	Enter the number of the restriction/permission list you want to apply to this class of service in the AMIS Open Networking Restriction/Permission List field.

Note: The name of the restriction/permission list will not appear until the cursor is off the field or the changes have been saved.

Step	Action
7	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Section J: Controlling access to Meridian Mail mailboxes

In this section

Overview	7-124
Using the Voice Security Options screen	7-125
Default security settings	7-131
Initial password change	7-133
Password display suppression	7-135
Password prefix	7-136
Password length	7-138
Forced regular password changes	7-139
Invalid logon attempts	7-142
Modifying mailbox security settings	7-146
Restricting off-site access to mailboxes	7-147
Disabling unused mailboxes	7-148

Overview

Introduction

Mailboxes are a potential source of unauthorized system use if proper safeguards are not put in place.

The kind of damage a hacker can do

The damage a hacker can do depends on what has been accessed:

- A personal mailbox *without* thru-dial capabilities

  This causes minimal damage as the hacker has only gained access to the personal mailbox. In this case, the hacker would have access to all of the mailbox and message commands and could record obscene greetings, listen to messages, and so on.
- A personal mailbox *with* thru-dial capabilities

  This can cause significant damage to your PBX and Meridian Mail system, especially if the hacker is able to break in to the system.
- The business or Meridian Mail system

  This can cause significant damage to your PBX and Meridian Mail system since this mailbox usually allows users calling in access to the thru-dial feature.

Proactive mailbox security measures

Meridian Mail provides four ways that you can control the level of security for users' mailboxes:

1. Use the password prefix and increase the minimum password length to make passwords harder to guess.
2. Force users to change their passwords regularly.
3. Control the number of maximum invalid logon attempts.
4. Disable external logon to mailboxes (when the highest level of security possible is required).

Using the Voice Security Options screen

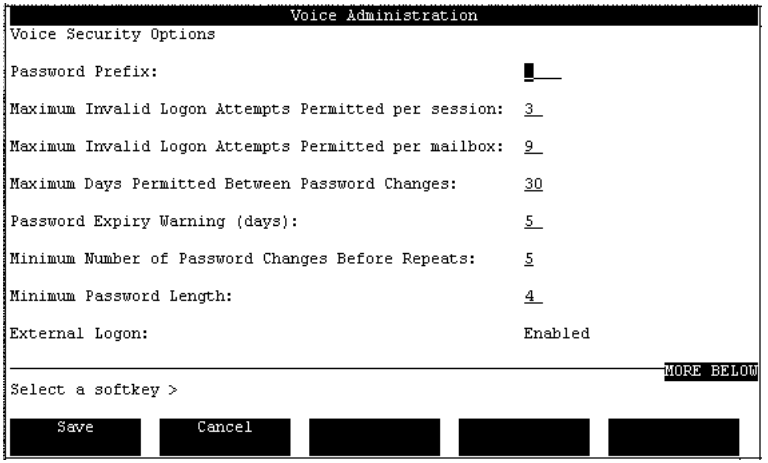
Introduction

The Voice Security Options screen allows you to control various security features and set restriction and permission codes that can be applied to features such as call answering, call sender, Express Messaging, mailbox Thru-Dial, and AMIS networking

Voice Security Options screen

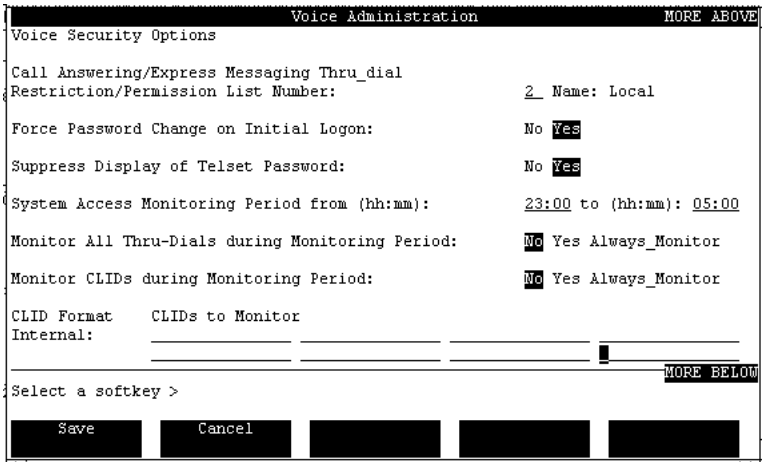
Part 1

This is the first part of the Voice Security Options screen.


Voice Administration
Voice Security Options
Password Prefix:
Maximum Invalid Logon Attempts Permitted per session: 3
Maximum Invalid Logon Attempts Permitted per mailbox: 9
Maximum Days Permitted Between Password Changes: 30
Password Expiry Warning (days): 5
Minimum Number of Password Changes Before Repeats: 5
Minimum Password Length: 4
External Logon: Enabled
MORE BELOW
Select a softkey >
Save
Cancel

Part 2

To view the additional fields in part 2 of the screen, press the <Page down> key or the down arrow.



Field descriptions

The following fields are used to protect mailboxes against unauthorized use. The fields used to monitor mailbox access can be found in Section K: Monitoring access to Meridian Mail mailboxes and features.

Password Prefix	
Description	The Password Prefix is a set of (up to four) digits that is inserted at the start of the default mailbox password whenever you create a new mailbox.
Default	System-generated four-digit code
Maximum Length	4 digits The prefix plus the user's DN cannot exceed 16 digits.

Maximum Invalid Logon Attempts Permitted per Session	
Description	This is the maximum number of times a user or caller can enter an invalid password within one logon session.
Default	3
Valid Range	1 to 99

Maximum Invalid Logon Attempts Permitted per Mailbox	
Description	This is the number of maximum invalid passwords that can be entered for a mailbox. This does not apply to the current logon session only. The number of invalid logons are counted over time.
Default	9
Valid Range	1 to 99

Maximum Days Permitted Between Password Changes	
Description	This field determines how often users are forced to change their mailbox passwords.
Default	30
Valid Range	0 to 90 0 indicates users do not have to change passwords.
Dependencies	MMUI only

Password Expiry Warning (days)	
Description	When a user's password is about to expire, a warning is played to notify the user and give him or her the chance to change it before it expires. This field determines how many days before password expiry the warning is played.
Default	5
Valid Range	0 to 60 0 indicates that a warning will not be played.
Dependencies	MMUI only Displayed when the maximum days between password changes is one or greater.

Minimum Number of Password Changes Before Repeats	
Description	This field determines the number of different passwords that must be used before the same password can be reused.
Default	5
Valid Range	0 to 5 0 indicates that users can reuse the same password.
Dependencies	MMUI only Displayed when the maximum days between password changes is one or greater.

Minimum Password Length	
Description	This is the minimum number of digits required in passwords that are entered from the telephone keypad. This includes mailbox passwords and access and update passwords for voice services.
Default	4
Valid Range	4 to 16
Dependencies	MMUI only.

External Logon	
Description	This feature is usually enabled to allow users to log on to their mailboxes from remote off-switch phones.This feature can be disabled to provide maximum security. When disabled, users cannot log on to their mailboxes from off-switch phones.
Default	Enabled
To disable	Call your Nortel distributor to disable this feature.
Valid Options	Enabled, Disabled
Dependencies	MMUI only

ATTENTION

Once disabled, this feature can never be reenabled.

Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number

Description	This field indicates which Restriction/Permission List should be applied to Call Answering/Express Messaging Thru-Dials.
Default	None

Force Password Change on Initial Logon

Description	This field compels users who are logging in to their mailbox for the first time to immediately change the default password.
Default	Yes
Dependencies	This field is displayed only if the interface is MMUI.

Suppress Display of Telset Password

Description	This field suppresses the display of password digits by replacing them with dashes on telephones with displays.
Default	Yes
Dependencies	None

System Access Monitoring Period from (hh:mm)

Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00

Monitor All Thru-Dials during Monitoring Period	
Description	This field indicates whether all Thru-Dial services (from a mailbox, voice menu, or directly from a VSDN) are to be monitored, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

Monitor CLIDs during Monitoring Period	
Description	This field indicates whether calling line IDs (CLIDs) are to be monitored during logon or by the Thru-Dial service, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

CLID Format—Internal—CLIDs to Monitor	
Description	These are the internal CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

CLID Format—External—CLIDs to Monitor	
Description	These are the external CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

Default security settings

Purpose

On a newly installed system, the security parameters are configured with default settings. These defaults may be appropriate for your system. If this is the case, you will not have to modify the settings.

However, the default settings may not adequately secure your Meridian Mail system to meet your business requirements.

Security checklist

Review the checklist below to determine if you need to change any of the default values that are assigned to passwords. You can also fill in this checklist with your new settings.

Information about these parameters is provided on the following pages.

Parameter	Default value
Password Prefix	4-digit code
Maximum Invalid Logon Attempts Permitted per Mailbox	9
Maximum Invalid Logon Attempts Permitted per Session	3
Maximum Days Permitted Between Password Changes	30
Password Expiry Warning (days)	5
Minimum Number of Password Changes before Repeats	5
Minimum Password Length	4
External Logon	Enabled
Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number	None
Force Password Change on Initial Logon	Yes
Suppress Display of Telset Password	Yes

Parameter	Default value
System Access Monitoring Period from (hh:mm)	23:00 to 05:00
Monitor All Thru-Dials during Monitoring Period	No
Monitor CLIDs during Monitoring Period	No
CLID Format—Internal—CLIDs to Monitor	None
CLID Format—External—CLIDs to Monitor	None

Initial password change

Introduction

Another measure to enhance security is to ensure that users change their initial password. This way, unauthorized access is prevented by those who may know the password prefix and mailbox number.

The initial password change feature provides the ability to force users to change their password the first time they log in.

How it works

When users log in to their mailbox for the first time, their default password is treated as "expired," and they are forced to change their password at this time.

Note: When a user enters his or her password for the first time, and any time thereafter, it is not displayed on the telephone set display. For more information on this feature, see "Password display suppression" on page 7-135.

This feature is enabled for all systems.

This feature only applies to MMUI mailboxes including Hospitality staff users. For VMUIF systems, this feature will be disabled, and it will not apply to hospitality guest users.

Enforcing an initial password change

To ensure that new users are forced to change their passwords when they log in for the first time, use the following procedure.

Step	Action
1	Select Voice Administration from the Main Menu. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Select Yes in the Force Password Change on Initial Logon field.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password display suppression

Introduction

The password display suppression feature prevents display of entered password digits on telephone sets that have display screens. This prevents “shoulder surfers” from seeing your password.

How password display suppression works

When users enter their passwords, each digit in the password is replaced by a dash (-). The pound (#) key continues to be displayed as #, but the star (*) key is displayed as a dash if the feature is enabled.

This feature is not supported for external calls because the local switch has no control on the suppression capability.

Suppressing the display

To suppress the display of password each time a user logs in to Meridian Mail, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Select Yes in the Suppress Display of Telset Password field.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password prefix

Introduction

When a new mailbox is created, the default password is the user's extension number. Until the user changes the default password, this may be a potentially serious security risk.

Password prefix

A password prefix provides another level of security by appending a short code before the default password. This code can be between two to four digits in length.

When a password prefix is defined, it is inserted at the beginning of the default mailbox password—the prefix is only inserted for new mailboxes.

Example
If mailbox 2339 is created and a password prefix of 34 has been defined, then the mailbox user will enter 342339 as the password the first time he or she logs in to Meridian Mail.

How prefixes work

The password prefix only applies to new MMUI users regardless of whether it is being defined for the first time or has been changed. VMUIF users continue to have their default password set to null and must log in from their "home phone" to change their password.

The password prefix applies only until the user changes the password. For example, when the user of mailbox 2339 changes the password for the first time, the prefix is no longer required.

Guidelines

Change the password prefix on a regular basis for maximum security. When you change the password prefix, it does not affect existing mailboxes, only newly created mailboxes.

Setting up the password prefix

To apply a password prefix, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Enter the prefix in the Password Prefix field. **Note:** The combined password prefix and the actual password cannot exceed 16 digits in length.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password length

Introduction

The length of the password, in conjunction with other mailbox features, can make it very difficult for hackers to break into your Meridian Mail system. You should never depend on one feature alone to safeguard your system.

Note: The password length feature only applies to MMUI systems.

How having a long password increases security

A long password increases your security provided that the password and the mailbox number are *not* the same. Having a long password means that there are more combinations to enter which could discourage the hacker.

Defining the password length

To define the minimum password length, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the password length in the Minimum Password Length field. **Note:** The password length including the password prefix cannot exceed 16 digits in length.
4	Do you want to save the configuration?

IF	THEN press
Yes	[Save].
No	[Cancel].

Forced regular password changes

Introduction

Forced password changes help increase security especially if they are done regularly. By compelling mailbox users to change their passwords and encouraging them to vary the length, it makes it very difficult for hackers to guess your password patterns.

Who can change the password

The mailbox password is changeable by both the administrator and the mailbox user. It can be altered as often as desired.

Relevant fields

The following fields in the Voice Security Options screen are related to forced password changes. The second and third fields are displayed only if the first field is set to a value of 1 or more:

- Maximum Days Permitted Between Password Changes
- Password Expiry Warning (days)
- Minimum Number of Password Changes before Repeats

Note: These fields apply to the MMUI interface only.

For more information on the Voice Security Options screen and its fields, see "Modifying mailbox security settings" on page 7-146.

Maximum days between password changes

You can either force users to change their passwords on a regular basis, or you can allow them to change them when or if they want.

Default

On a newly installed system, the default setting forces users to change their passwords every 30 days. You can choose a value between 0 and 90 days.

Guideline

Forcing users to change their passwords on a regular basis is recommended since this results in a much greater level of security.

Expired passwords

If a user's password expires, the user is not allowed to retrieve messages until he or she changes the password.

> **ATTENTION**
>
> If you change this value from 0 to another value on an operational system, user passwords expire immediately. Make this change during a slow traffic time and inform users of the change. After the change, you may notice a number of 3134 DR SEERs that indicate users did not change their passwords when prompted.

Password expiry warning

If the maximum days between password changes is set to 1 or more, you can play an expiry warning message to users before their password is about to expire. This warning reminds the user that the password is going to expire in X days and gives the user the chance to change the password before it expires.

This field gives you control over when this password is played.

WHEN this field is set to	THEN the warning will
a value between 1 and 60	be played this many days before the password is set to expire.
0	not be played. When the user's password expires, he or she will be prompted for a new password at logon.

Minimum password changes before repeats

To further increase mailbox security, you can force users to use a different password whenever their password expires. Otherwise, users may simply enter the same password over and over every time their password expires.

This setting is not applicable if the maximum days permitted between password changes is zero (0).

Enforcing regular password changes

To set up your system so that mailbox users will have to change their passwords, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the expiration period in the Maximum Days Permitted Between Password Changes field. **Note:** The valid range is from 0 to 90 days and the default is 30. If you set this field to 0, the users are not forced to change their password and you do not have to configure any other fields. In this case, go to step 6 to save or cancel the changes.
4	Set the number of days of advance notice that users will hear before their password expires in the Password Expiry Warning (days) field.
5	Set the number of passwords that have to expire before a user can reuse an old password in the Minimum Number of Password Changes Before Repeat field.
6	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Invalid logon attempts

Introduction

The Invalid Logon Attempts feature allows you to define the number of times, within a range of one to nine, that a caller can enter an invalid logon password for a mailbox before the system disables the mailbox. Once the mailbox is disabled, only the system administrator can reenable it at the administration terminal. When a mailbox is disabled, Meridian Mail still takes and stores incoming messages but does not permit logons.

The feature is useful in preventing hackers from entering one password after another until they gain access to a mailbox.

The feature also allows you to specify the number of invalid logon attempts per session as well as per mailbox. This discourages hackers from hopping around from one mailbox to another, disabling them with invalid logon attempts.

Relevant fields

There are two fields in the Voice Security Options screen that control the number of allowable invalid logon attempts:

- Maximum Invalid Logon Attempts Permitted per Session
- Maximum Invalid Logon Attempts Permitted per Mailbox

For more information on the Voice Security Options screen and its fields, see “Modifying mailbox security settings” on page 7-146.

Invalid logons per session

This field determines how many invalid passwords can be entered in a row during one logon session. If this limit is reached, the logon session is terminated.

Example

If a hacker knows your Meridian Mail access code and some DNs, this is what would happen if your maximum invalid logon attempts per session were set to 3.

Attempt	Description
1	The hacker tries logging in to mailbox 2498 but enters an incorrect password.
2	The hacker tries logging in to mailbox 2498 again but enters an incorrect password.
3	The hacker tries logging in to mailbox 2475 but enters an incorrect password.
	The logon session is terminated.

Invalid logons per mailbox

Meridian Mail also keeps track of how many invalid logon attempts have been made on each mailbox. This does not apply to the current logon session only. The number of invalid passwords entered is counted over time.

The counter is reset to 0 when the user changes the password.

If the limit is reached, the mailbox is disabled. Meridian Mail still takes and records incoming messages, but does not allow the user to log on.

Disabling a mailbox

To specify how many invalid logon attempts will be allowed before a mailbox is disabled, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the number of invalid logon attempts per session in the Maximum Invalid Logon Attempts Permitted per Session field. The valid range is from 1 to 99, and the default is 3.
4	Set the number of invalid logon attempts per mailbox in the Maximum Invalid Logon Attempts Permitted per Mailbox field. The valid range is from 1 to 99, and the default is 9.
5	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Reenabling an MMUI mailbox

To reenable a disabled MMUI mailbox, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Choose User Administration.
2	Choose Local Voice User.
3	Do you know the user's DN?

IF	THEN
yes	press [View/Modify]. Enter the user's DN and press <Return>. Go to step 9.
no	follow step 4 to step 8.

Step	Action
4	Press [Find] to do a search.
5	Specify the criteria for the search.
6	Press [List].
7	Position the cursor beside the user you want to modify and press the spacebar to highlight the entry.
8	Press [View/Modify].
9	Move the cursor to the Logon Status field.
10	Select Enabled.
11	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Reenabling a VMUIF mailbox

The setting in the Mailbox Lockout Duration field determines how a VMUIF mailbox has to be reenabled. This field is located in the View/Modify Class of Service screen. The duration is specified in hours and minutes (hh:mm).

WHEN the lockout duration is	THEN
00:01 or greater	the mailbox will be automatically reenabled after the specified time.
00:00 (zero)	you must manually reenable the mailbox in the Logon Status field in the View/Modify Local Voice User screen. The procedure is the same as “Reenabling an MMUI mailbox” on page 7-144.

Modifying mailbox security settings

When to use

Follow this procedure

- after installation, if some or all of the default settings do not meet your organization's requirements
- to change the current settings to reflect a new security policy or tougher security measures

Procedure

To modify current mailbox security settings, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Modify some or all of the following fields to meet your security requirements: • Password Prefix • Maximum Invalid Logon Attempts Permitted per Session • Maximum Invalid Logon Attempts Permitted per Mailbox • Maximum Days Permitted Between Password Changes • Password Expiry Warning • Minimum Number of Password Changes before Repeats • Minimum Password Length • Force Password Change on Initial Logon • Suppress Display of Telset Password For more information, see the appropriate topics.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Restricting off-site access to mailboxes

Introduction

External logon is enabled by default, allowing users to log on to their mailboxes from phones that are external to the switch. If security is of the highest priority, Meridian Mail provides a facility allowing the system to restrict access to a mailbox from an offsite location.

Implementing this feature

This feature (SW7007) can be ordered from a Nortel sales representative and is implemented by authorized field technicians.

ATTENTION

Once the external logon feature is disabled on the system, it can *never* be reenabled.

Disabling unused mailboxes

Introduction

Whenever employees are terminated, you should immediately disable their mailbox. This prevents them from abusing your system by billing toll calls to your company.

You should make arrangements with your Personnel department to inform you of terminations so you can disable system access.

Procedure

To disable an unused mailbox, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press [View/Modify], and then enter the local voice user. If you do not know the local voice user, do the following: a. Press the [Find] softkey followed by the [List] softkey. b. Position the cursor beside the user you want to view or modify, and press the [SpaceBar]. c. Press [View/Modify].
4	Position the cursor on the Logon Status field.
5	Set the field to Disabled to disable the mailbox.
6	Press [Save] to save the configuration.

Section K: Monitoring access to Meridian Mail mailboxes and features

In this section

Overview	7-150
Hacker Monitor	7-151
Mailbox Login Monitoring	7-152
Thru-Dial Monitoring	7-154
CLID Monitoring	7-158
The Services Summary Traffic report	7-161

Overview

Introduction

This section of the chapter describes the reports and features in Meridian Mail intended to assist you in identifying attempts to violate the security of your system.

These include the following:

- the Services Summary Traffic report
- the Hacker Monitor feature
- mailbox login monitoring
- Thru-Dial monitoring
- CLID monitoring

Hacker Monitor

Introduction

This feature enables you to monitor selected or all mailbox logins and Thru-Dials, which helps you to check for activity on your system that may indicate the presence of hackers.

When this feature is combined with the SEER Mailbox feature, you can be notified through Remote Notification when a suspected unauthorized user attempts a Thru-Dial or enters a particular mailbox.

Description

The Hacker Monitor capability is provided by three different methods:

- by monitoring mailbox logins (see "Mailbox Login Monitoring" on page 7-152)
- by monitoring the use of Thru-Dial services (see "Thru-Dial Monitoring" on page 7-154)
- by monitoring mailbox logins or attempted Thru-Dials from specified calling line identification numbers (CLIDs) (see "CLID Monitoring" on page 7-158)

Mailbox Login Monitoring

Introduction

Possible hacker activity may be detected by monitoring mailbox logins of requested local voice users.

How to do it

You use the System Access Monitoring Period field on the Voice Security Options screen and the Monitor Mailbox during Monitoring Period field on the Local Voice User screen to set up mailbox login monitoring.

Field descriptions

This table describes the fields that are used to set up mailbox monitoring.

System Access Monitoring Period	
Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logins for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 5:00 Both the start and the end time for this period are specified in the hh:mm format using the 24-hour clock.
Monitor Mailbox during Monitoring Period	
Description	When this field is set to Yes, all logins into the mailbox during the system access monitoring period will result in SEER 2262 being issued for MMUI users or SEER 5662 being issued for VMUIF users.
Default	No
References	For more information on local voice users, see Chapter 9, “Local voice users”.

Administration level

You can monitor a mailbox from either the System Administration level or the Customer Administration level.

Procedure

To monitor mailbox logins, follow these steps.

Starting Point: The Meridian Mail Main Menu or the Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Specify a time interval in the System Access Monitoring Period field.
4	Press [Save].
5	Return to the Customer Administration menu.
6	Select User Administration.
7	Select Local Voice Users.
8	Select the local voice user you want to modify or add. For more information on modifying or adding local voice users, see Chapter 9, “Local voice users”.
9	Set the Monitor Mailbox during Monitoring Period field to Yes.
10	Press [Save].

Thru-Dial Monitoring

Introduction

Possible hacker activity may be detected by monitoring selected or all Thru-Dial services used either during the system access monitoring period or at all times.

How to do it

Use the Voice Security Options screen and the Thru-Dial Definition screen to set up Thru-Dial Monitoring.

Note: The monitoring period is determined by the values entered in the System Access Monitoring Period from (hh:mm) field on the Voice Security Options screen.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Thru-Dial Definition screen
all Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor	no action is required.
specified Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to No	for the desired service, set the Monitor this Service during Monitoring Period field to Yes.

Field descriptions

You will find descriptions of the Voice Security Options fields on page 7-125. For descriptions of the fields in the Thru-Dial Definition screen, see Chapter 27, “Class of Service administration”.

Field descriptions (cont'd)

The following table only describes those fields which are used to set up Thru-Dial monitoring.

System Access Monitoring Period from (hh:mm)	
Description	This field indicates the monitoring period during which one or all of the following will be monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00
Available on	Voice Security Options screen

Monitor All Thru-Dials during Monitoring Period	
Description	When this field is set to Yes, all accesses to the Thru-Dial service (from a mailbox, voice menu, or directly from a VSDN) during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user. When this field is set to Always_Monitor, any access to the Thru-Dial service at any time will result in a class 106 informational SEER.
Default	No
Available on	Voice Security Options screen

Monitor this Service during Monitoring Period	
Description	When this field is set to Yes, all accesses to this Thru-Dial service during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user.
Default	No
Available on	Thru-Dial Definition screen

Administration level

You can monitor all Thru-Dials from either the System Administration level or the Customer Administration level.

Monitoring all Thru-Dials

To monitor all Thru-Dials, follow these steps.

Starting Point: The Meridian Mail Main Menu or the Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor.

IF you have set this field to	THEN go to
Yes	step 4.
Always_Monitor	step 5.

Step	Action
4	Set the monitoring period in System Access Monitoring Period from (hh:mm) field.
5	Press [Save].

Monitoring specific Thru-Dials

To monitor a specific Thru-Dial, follow these steps.

Starting Point: The Meridian Mail Main Menu or the Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor all Thru-Dials during Monitoring Period field to No.
4	Set the monitoring period in System Access Monitoring Period from (hh:mm) field.
5	Press [Save].
6	Go to the Thru-Dial Definitions screen.

Step	Action
7	Select the thru-dial definition you want to modify or add. Fore more information on thru-dials, refer to the *Voice Services Application Guide* (NTP 555-7001-325).
8	Set the Monitor this Service during Monitoring Period field to Yes.
9	Press [Save].

CLID Monitoring

Introduction

Possible hacker activity may be detected by monitoring mailbox logins or thru-dials that have been attempted from a specified calling line ID (CLID).

You can specify the type of CLID (Internal or External) and a string of digits (up to 15) of a CLID. That is, you can specify the complete CLID, the area code only, or the area code and office code. Up to 12 CLIDs can be entered for each type of CLID format. For more information on CLID, see Chapter 18, "Dialing translations".

How to do it

Use the Voice Security Options screen to set up CLID Monitoring.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Voice Security Options screen
CLIDs	set the Monitor CLIDs during Monitoring Period field to Yes or Always_Monitor	enter the numbers in the CLIDs to Monitor field.

Monitoring a subset of a CLID

If a subset of a CLID is to be monitored (an office code, for instance), this string of digits will be compared only to the beginning of the CLID and not with the number. Thus, if you want to monitor the office code, you must also specify the area code.

Remote notification of mailbox logons

When this feature is combined with the SEER Trigger Message feature, you can be notified through Remote Notification when a suspected unauthorized user attempts to access Thru-Dial or enters a particular mailbox.

Field descriptions

The following table only describes those fields which are used to set up CLID monitoring. For descriptions of all the Voice Security Options fields, see "Using the Voice Security Options screen" on page 7-125.

Monitor CLIDs during Monitoring Period	
Description	This field indicates whether CLIDs are to be monitored by the Voice Messaging Service during login or by the Thru-Dial service. This field also indicates when this monitoring should take place. When this field is set to No, CLIDs are not monitored, even if there are entries in the CLIDs to Monitor field. When this field is set to Yes, CLIDs are monitored during the system access monitoring period only. When this field is set to Always_Monitor, CLIDs are monitored at all times.
Default	No

CLIDs to Monitor	
Description	You can enter up to 12 CLIDs. These CLIDs are monitored by Voice Messaging on mailbox login or by the Thru-Dial service if the Monitor CLIDs during Monitoring Period is set to Yes or Always_Monitor.
Maximum length	CLIDs can be up to 15 digits in length.
Format	You can enter complete CLIDs, area codes only, or area codes and office codes. Do not include any dialing prefixes, such as ESN prefixes, in the numbers you enter.
Examples	4165551234 is a complete CLID. 416 is an area code. All CLIDs from this area code are monitored. 416555 is an area code and exchange code. All CLIDs in the 555 exchange in the 416 area code are monitored.
Default	None

SEERs issued

An informational SEER is issued if the CLID of a caller matches one of the numbers specified in the Voice Security Options screen during a mailbox login or Thru-Dial access. The informational SEERs can be 5562, 2262, or 10612. For more information on SEERs, refer to the *Maintenance Messages (SEERs)* (NTP 555-7001-510).

Administration level

You can monitor calling line IDs from either the System Administration level or the Customer Administration level.

Procedure

To monitor calling line IDs, follow these steps.

Starting Point: The Meridian Mail Main Menu or the Customer Administration Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor CLIDs during Monitoring Period field to Yes or Always_ Monitor.

IF you have set this field to	THEN go to
Yes	step 4.
Always_Monitor	step 5.

4	Set the monitoring period in the format hh:mm.
5	Enter the internal CLIDs to be monitored in the CLID Format—Internal block.
6	Enter the external CLIDs to be monitored in the CLID Format—External block.
7	Press [Save].

The Services Summary Traffic report

Introduction

This report provides statistics for each of the voice services installed on your system. It records the number of times a user dials a service (the number of accesses) during the reporting period and the average length of each access. The report records both direct and indirect accesses.

Direct accesses occur when a user dials the DN of the menu, announcement, or fax item.

Indirect accesses occur when a service is accessed from another service through a menu selection or a time-of-day controller.

For more information, see “Services Summary report” on page 32-12.

Report availability

This report is available on all systems.

Report frequency

Run this report regularly to check for unusually long Thru-Dial sessions or for unusual numbers of after-hours Thru-Dial sessions. These may be a sign that hackers are present on your system.

What to do

If you suspect hackers are accessing the Thru-Dial feature, first check how the Thru-Dial service is set up to see whether the Operational Measurements (OM) data are unusual. For example, if executives call in and access a Thru-Dial service, then you can expect an average number of calls. If this average is exceeded, it may be an indication of hacker activity.

If your research still suggests the presence of hackers, review the dialing restrictions for Thru-Dial. For details, refer to the *Voice Services Application Guide* (NTP 555-7001-325).

If you are using an access password for Thru-Dial, change the access password, and continue to monitor the Thru-Dial usage.

Section L: Equipment security

In this section

Overview	7-164
Switchroom access	7-165
Administration terminals	7-166
Meridian Mail and switch printouts	7-167

Overview

Introduction

This section of the chapter discusses security measures that you should exercise to safeguard the Meridian Mail and switch hardware.

General security measures

The following is a list of general security measures you can take to secure your Meridian Mail and PBX:

- Limit access to your switchroom and escort all visitors.
- Keep a list of authorized technicians on hand. Whenever a regular technician appears, ask for ID to ensure that he or she is still employed by the company.
- Establish procedures for temporary technicians. Ask the technician for ID and to sign in, and issue a visitor's badge. If the technician does not have a company ID, check with the company to ensure that the person is a valid employee.

Switchroom access

Introduction

When a switchroom is not secure, criminals can gain access to all your system resources. Their activity can be as benign as turning off printers or as malicious as removing cards from your switch and rendering your system inoperable.

Security measures

The following is a list of safety measures you should exercise:

- Physically lock the room in which your equipment is located.
- Use combination locks—hardkey locks can easily be broken. Nortel recommends using an electronic key and program to safeguard your equipment room.
- Change the combination regularly and only inform those who need to know the new combination.

Administration terminals

Introduction

There are two facilities provided for protecting against unauthorized access to the Meridian Mail administration terminal:

- the administration password
- hardware-based remote access restriction

Administration password

The administration terminal is password protected. When Meridian Mail is first installed, there is a default password. The first time you log on to the Meridian Mail administration terminal, you are forced to change this default password. You are recommended to change this password on a regular basis to maximize system security.

Passwords can be between 1 and 16 characters in length. However, it is recommended that the password be no less than seven characters in length. The longer the password, the less likely it is that someone will guess it.

Always log off before you leave the administration terminal, even if only for a short period.

Remote access restriction

If remote access is enabled on your system, anyone can dial in and commandeer your system. Remote access should not be enabled unless required (for example, for remote support personnel to work on your system).

Modular Option EC (ModOpEC) systems have an internal modem which is enabled using the <Ctrl> <w> key sequence. When a remote access session is in progress, local access is prohibited.

Non-EC systems are configured with an A/B switchbox between the terminal and the modem. When the switch is set to the modem setting, the system can be remotely accessed (but not from the local terminal). When the switch is set to the terminal setting, access is only possible from the local terminal. The switch is controllable at the site and must be switched manually.

Meridian Mail and switch printouts

Introduction

"*One man's garbage is another man's treasure.*"

Anonymous

This is very true for the telecommunication criminal known as the "dumpster diver." These divers search through your garbage looking for printouts or records of your system's codes.

Security measures

Do not throw out call detail records and credit card receipts. Dispose of these materials, including switch printouts and old documentation, as you do any proprietary materials.

Chapter 8

User administration—an overview

In this chapter

Section A: Introduction to User Administration	8-3
Section B: New user planning	8-13

Section A: Introduction to User Administration

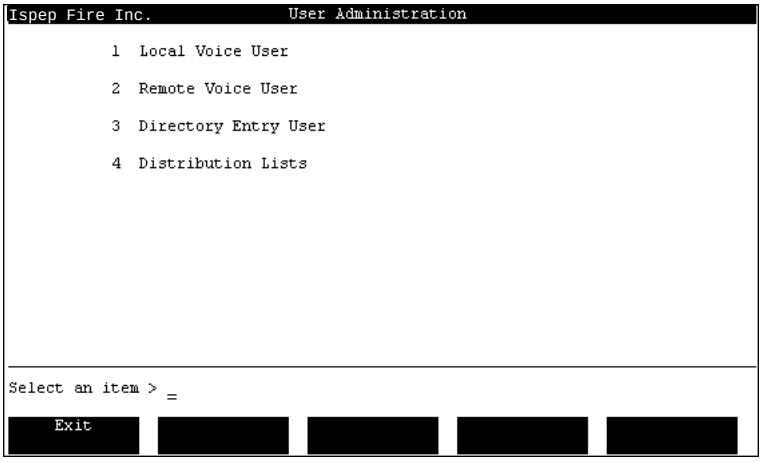
In this section

The User Administration menu	8-4
Types of users	8-6
Distribution lists	8-9
Limitations and guidelines	8-10
Support for multiple appearance DNs	8-11

The User Administration menu

The User Administration menu

This is the User Administration menu, the starting point for all user administration tasks. In this example of the screen, Meridian Networking is installed.



Local Voice User

This menu item allows you to add, view, modify, and delete local voice users. Local voice users have mailboxes on your local Meridian Mail site.

Remote Voice User

This menu item is displayed if the Meridian Networking feature is installed. It allows you to add, view, modify, and delete remote voice users. Remote voice users are users at remote sites that are added to your local site's database.

Directory Entry User

This menu item allows you to add, view, modify, and delete directory entry users. Directory entry users do not have mailboxes.

Distribution Lists

This menu item allows you to add, view, modify, and delete distribution lists. Distribution lists are used to send messages to a number of people.

Related chapters

This table directs you to the chapters that contain information about each of the items in the User Administration menu.

For the following option	Refer to
Local Voice User	Chapter 9, “Local voice users”
Remote Voice User	Chapter 10, “Remote voice users”
Directory Entry User	Chapter 11, “Directory entry users”
Distribution Lists	Chapter 12, “Distribution lists”

Types of users

Three types of users

There are three types of users that you can add to Meridian Mail:

- local voice users
- remote voice users
- directory entry users

Local voice users

Local voice users have extensions on the local switch.

Local voice users have mailboxes with call answering and voice messaging capability. This means the following:

- If the user is away from his or her phone, callers are forwarded to the user's mailbox to leave a message.
- The user can compose and send voice messages to other users.

Voice Messaging interfaces

There are three Voice Messaging interfaces. Each customer can only use one of the installed interfaces. This is set up when the customer is added.

Interface	Description
MMUI	This is full-featured Voice Messaging that provides users with call answering and voice messaging capabilities.
VMUIF	This is a call answering interface intended for users who primarily need call answering capability only (although compose capability can be enabled in users' classes of service).
Hospitality	This interface is intended for the hospitality industry and is available only if Hospitality Voice Messaging is installed. It provides two specialized interfaces: one for guests and one for staff.

Remote voice users

Users can be added as remote voice users only if the Meridian Networking feature is installed.

When you add a user who is located at a remote Meridian Mail site as a remote voice user, you are adding that user to your local user database.

Benefits

The benefits of adding users at remote sites to your local site's database as remote voice users are as follows:

- Whenever a user at the local site addresses a message to a remote voice user, the remote voice user's personal verification (spoken name) is played.
- Local users can use Name Dialing and Name Addressing to call and compose messages to remote voice users.
- While listening to a message left by a remote voice user, a local user can use Call Sender (press 9 on the keypad) to immediately call back the originator of the message.
- External callers can name-dial remote voice users (if this feature is enabled).
- Remote voice users can be added to distribution lists.

Types of remote voice users

There are two types of remote voice users.

User type	Description
Permanent	Permanent users remain on the system until you delete them using User Administration.
Temporary	If the number of temporary users exceeds the maximum, those who have not been active for a long time are automatically deleted by the system during nightly audits.

Directory entry users

Directory entry users are registered in the Meridian Mail directory. However, they do not have mailboxes. This means that they do not have access to call answering or voice messaging capability.

They can, however, be reached by features such as Name Dialing and Thru-Dialers.

Example

You have added Rupert Hewison as a directory entry user. If he does not answer his phone, callers are not forwarded to Meridian Mail in order to leave a message. He also cannot compose and send voice messages to other users.

However, when a caller accesses a thru-dial service and enters Rupert's extension (or name, if name dialing is used), his phone rings.

Distribution lists

Description

A distribution list is a list of mailbox numbers. When you enter the distribution list number during message composition, the message is sent to all of the mailbox numbers in the list.

Distribution lists, therefore, make it easier and quicker to address messages to groups of people. Once the distribution list has been created, you only need to enter one number during message composition (the distribution list number).

Personal versus system distribution lists

Users can create their own distribution lists from the telephone set. These are known as personal distribution lists.

The distribution lists that you create through User Administration are system distribution lists, and are created and maintained by the system administrator, not users.

You can add up to 120 mailbox numbers to a system distribution list. Users can add up to 99 mailbox numbers to personal distribution lists.

Limitations and guidelines

Multiple Administration Terminals

If the Multiple Administration Terminals (MAT) feature is installed, you can perform User Administration from a secondary terminal.

If more than one administrator accesses a user or distribution list at the same time, the administrator who first gained access to the user or list can modify the information. The other administrator can only view the information (no [Save] softkeys are displayed in the User Administration screens).

Nightly audits

Meridian Mail performs a system audit every day at 2:30 a.m. This audit can take anywhere from ten minutes to two hours. The more changes that have been made to the system since the last audit, the longer the audit will take.

> **CAUTION**
>
> **Risk of Interrupted Service**
>
> Do not perform user administration during the nightly audit. Doing so may cause loss of service.

Support for multiple appearance DNs

Description: MADN

A Multiple Appearance DN (MADN) is a directory number (DN) that is programmed on several phone sets.

Usage

Multiple Appearance DNs are typically used in customer support environments in which you want to ensure that calls are answered. MADNs allow more than one call to be handled at a time.

How MADNs work

A call to a multiple appearance DN rings a number of phone sets, increasing the chances that the call will be answered.

The primary phone

The telephone set on which the MADN is programmed as key 0 is considered the primary phone.

Example

DN 5000 is programmed on four Meridian 1/SL-1 terminal numbers (TNs):

- DN 5000 is programmed as key 3 on TN 0-0-1-0.
- DN 5000 is programmed as key 4 on TN 0-0-5-7.
- DN 5000 is programmed as key 0 on TN 26-0-4-2. This is the primary phone.
- DN 5000 is programmed as key 1 on TN 26-0-4-3.

A call comes in to the customer support center. All four telephone sets ring.

When someone answers the call, the other phones stop ringing. When another call comes in on DN 5000, the three remaining telephone sets ring even though the first call is still in progress.

How Meridian Mail treats MADNs

Multiple appearance DNs are treated as one DN by Meridian Mail. How the primary phone is programmed determines what happens to a call when it is not answered in the predetermined number of rings or when all telephones are busy.

Programming requirement

The primary phone must be programmed to forward to the voice messaging DN on busy and no answer conditions. Otherwise, calls will not get forwarded to Meridian Mail when all telephone sets are busy or when a call goes unanswered.

Section B: New user planning

In this section

Overview	8-14
Class of service planning	8-15
Distributing local voice users evenly over volumes	8-17
Guidelines for adding users to a system that has disk shadowing	8-19
Guidelines for adding a large number of users	8-20
How user models in pre-Release 9 systems are converted to classes of service	8-21

Overview

Introduction

This section describes how to plan the task of adding users to a newly installed system.

Planning tasks

Before you begin adding users to your system, you should do the following.

1. Identify the types of users that you will be adding to the system.

   Will you be adding remote voice users or directory entry users, or both, in addition to local voice users?
2. Classify local voice users into categories that serve as the basis for your classes of service.

   See “Class of service planning” on page 8-15.
3. If you have disk shadowing on some nodes but not on others, identify which local voice users should be put on the shadowed nodes.

   See “Guidelines for adding users to a system that has disk shadowing” on page 8-19.
4. If you are adding a large number of users (600 or more) within a 24-hour period, review the guidelines on page 8-20.

Class of service planning

Introduction

Classes of service (COSs) act as templates to simplify the process of adding and maintaining local voice users.

When you create a class of service, you specify three types of information about the users to which the class of service will be assigned:

- which features are enabled/disabled
- limitations and attributes
- which restriction/permission lists are applied to certain features

When you assign a class of service to a user, all of the attributes defined in the class of service are applied to the user.

When you modify a class of service, all users who are assigned to that class of service are immediately updated.

Example

These are some of the features you can enable/disable in classes of service:

- Delivery to Non-User
- Remote Notification
- AMIS Networking

These are some of the limitations and attributes you can specify:

- maximum lengths for composed and call answering messages
- maximum voice storage limit
- how long read messages are stored before being deleted
- whether invalid personal distribution list addresses are automatically deleted

You can assign restriction/permission lists to features such as

- Extension Dialing
- External Call Sender
- Custom Revert

When to create classes of service

Because each local voice user must be assigned to a class of service, classes of service must be defined before you begin adding local voice users to your system.

Classifying users

Classify your users into types, and then create classes of service that meet the needs and requirements of each type.

Example

You might create classes of service for different departments or jobs, or both, that have different usage profiles and requirements:

- Sales
- Engineering
- Marketing
- Manager
- Secretary

See also

For more information about classes of service, see Chapter 27, “Class of Service administration”.

Distributing local voice users evenly over volumes

Introduction

Meridian Mail systems can have from one to five nodes, each of which contains a hard disk drive for data storage. These disk drives are partitioned into volumes.

When you add a local voice user, the user must be assigned to a particular volume. This is where all user-related data and voice are stored, such as mailbox information, personal greetings, voice messages, and voice prompts.

User volumes

This table indicates user volume names and where they are distributed across the various nodes.

Number of Nodes

Node #

	1 Node	2 Nodes	3 Nodes	4 Nodes	5 Nodes
Node 1	VS2	VS2	VS2*	VS2*	VS2*
Node 2		VS202	VS202	VS202	VS202
Node 3			VS203	VS203	VS203
Node 4				VS204	VS204
Node 5					VS205

Note: The asterisk (*) indicates that the volume contains only voice prompts and is considered to be a system volume, not a user volume.

The default volume

When you press the [Add] softkey to enter the Add a Local Voice User screen, the volume that is selected as the default is the volume with the greatest amount of free space at that time. All users that you add during a single session are added to that volume by default, unless you specify otherwise.

When you exit the Add a Local Voice User screen and then reenter it, the system reassesses which volume has the most available space and that volume becomes the new default.

Recommendations

To guarantee an effective distribution of users, the following actions are recommended:

- Distribute local voice users across volumes randomly in such a manner that does not result in heavy users all being assigned to the same volume(s).
- Spread employees in the same department across a number of nodes (do not place them all on the same node). This way, if a node is taken out of service for troubleshooting, the entire department will not be affected.

Disk usage information

Monitor disk usage on a regular basis to ensure that user volumes do not fill up. This is done by generating the Disk Usage report.

For more information about the Disk Usage report, see "Disk Usage Detail report" on page 32-52 in Chapter 32, "Operational Measurements traffic reports."

Moving users from a full volume

If a volume becomes (nearly) full, you can use the Move User utility to move local voice users from one volume to another. This utility is accessible from the Tools menu.

Refer to *System Administration Tools* (NTP 555-7001-305) for details.

Guidelines for adding users to a system that has disk shadowing

Introduction

Disk shadowing is an optional feature that is available on the Modular Option EC platform. It provides protection against data loss in the event of disk failure.

How it works

This feature works by writing new information to two disks at the same time. If one disk fails, it is taken out of service without service interruption. Disks are shadowed on a node-by-node basis.

If a shadowed disk fails, voice messages of users on that node are not lost since they will be on the second disk of the shadowed pair.

Before you add users

Before adding users, you need to do the following.

1. Determine which nodes are shadowed and which are not.
2. Identify which users you want to put on shadowed nodes.

   Local voice users whose messages may not be critical can be placed on nonshadowed nodes.

Guidelines for adding a large number of users

Recommendation

Avoid adding a large number of users (1000 or more) within a 24-hour period. Every 24 hours, a nightly audit takes place between 2:30 a.m. and 5:00 a.m. When a large number of users is added between audits, the directory that stores user information can become unbalanced and perform less efficiently.

Guidelines

If you must add a large number of users between audits, follow these guidelines:

- Ensure that the number of local voice users to be added is within the engineering guidelines for the system.
- Add users in reverse alphabetical order.

  When you add users in alphabetical order, performance gradually degrades as you add more users. This degradation in performance is corrected when the next nightly audit occurs.
- Distribute local voice users across volumes as evenly as possible.
- If you add a lot of users who either belong to the same department or who have mailbox numbers beginning with the same numbers, the system will begin to slow down as you add more users. Therefore, try to add users in a more random fashion to avoid performance degradation.

System slowdown while adding users

If you notice that the system is slowing down as you add users, stop. You can force an audit from the Tools menu using the Rebalance Directory tool. However, do not force an audit during a busy traffic time. During a forced audit, you will not be able to add more users.

For more information about this utility, refer to *System Administration Tools* (NTP 555-7001-305).

How user models in pre-Release 9 systems are converted to classes of service

Introduction

Classes of service (COSs) replaced user models in Meridian Mail Release 9. Prior to Release 9, a user model was assigned to each user. However, if you modified the user model, it was changed for that user only. You could not propagate changes to a user model to all local voice users that were added using that model.

How user models are converted to COSs

When you convert to Meridian Mail 12 from a release prior to Meridian Mail 9, all existing local voice users are assigned to a personal class of service. This means that each user has a unique class of service that is not connected to any of the system classes of service. Therefore, local voice users must be reassigned to system classes of service after a conversion.

COS conversion utility

The COS Conversion utility is available from the Tools menu and should be used when converting from a system that used user models to one that uses classes of service.

For more information about this utility, refer to *System Administration Tools* (NTP 555-7001-305).

How it works

This utility checks each local voice user's personal class of service.

WHEN the personal COS	THEN
matches an existing system COS	the local voice user is assigned to the matching system COS.
does not match an existing system COS	the personal COS is used for that user.

How to use this utility

You can use the COS Conversion utility to do one or both of the following:

- View unassigned local voice users, and then create a system class of service based on the personal class of service.
- Assign unassigned users to defined system classes of service.

Chapter 9

Local voice users

In this chapter

Section A: Adding local voice users	9-3
Section B: Finding local voice users	9-43
Section C: Modifying and deleting local voice users	9-77

Section A: Adding local voice users

In this section

Integrated mailbox administration	9-4
Before you begin adding local voice users	9-5
Adding a local voice user	9-7
Accessing the Add Local Voice User screen	9-9
The Add Local Voice User screen	9-12
Entering user information	9-14
Assigning a user to a class of service	9-17
Primary DN and extension DNs	9-21
The revert DN	9-23
See “Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN” on page 9-29.	9-26
Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN	9-29
Recording a personal verification for a user	9-32
Creating a remote notification schedule for a user	9-34
Setting other local voice user characteristics	9-37

Integrated mailbox administration

Description

Integrated Mailbox Administration (IMA) is a feature that allows you to add mailboxes for users at the Meridian 1 terminal. This feature was introduced in Release 9.0 of Meridian Mail and Release 19 of X11. In X11, this feature is known as Voice Mailbox Administration (VMBA).

Other types of users

The following types of mailboxes and users cannot be added using VMBA and, therefore, must be added through User Administration in Meridian Mail:

- guest mailboxes (Hospitality voice messaging)
- remote voice users
- directory entry users

Fields you cannot change in User Administration

If you add mailboxes using VMBA, you cannot modify any of the following fields in Meridian Mail User Administration. These fields are controlled by VMBA on the Meridian 1.

X11 Field	Meridian Mail Field
DN	Mailbox Number, Primary DN
VMBA Class of Service	Class of Service
CPND Name	Last Name, First Name, Initials
Second DN	Second of the Extension DN fields
Third DN	Third of the Extension DN fields

If you change any of these fields in Meridian Mail, discrepancies may arise. Periodic audits are performed on the Meridian 1. During these audits, VMBA settings override any settings configured in Meridian Mail.

See also

For more information about the Integrated Mailbox Administration feature, see Appendix A, "Integrated Mailbox Administration".

Before you begin adding local voice users

Introduction

Before you begin adding local voice users, consider the following points.

Classes of service

All local voice users must be assigned to a class of service. Classes of service should be defined before you begin adding local voice users.

Have you created all of the necessary classes of services? If you have not, do the following:

- Create all the classes of service that you need.

  See Chapter 27, “Class of Service administration. ”
- Add the classes of service to the system.

  See “Assigning Classes of Service to customer groups” on page 27-51. Add the classes of service to customer groups.

Password for MMUI users

All MMUI users must have a password. When you add a new local voice user, the system assigns a default password (the user’s mailbox number).

To make this initial default password more secure, you can enter a password prefix in the Voice Security Options screen. This prefix is added in front of the user’s mailbox number to make initial passwords more difficult to guess.

Passwords for VMUIF users

A default password is not assigned to new VMUIF users. A VMUIF user that does not have a password can access Meridian Mail from his or her "home phone" only.

Users who want to be able to log in from any phone need a password. This includes users who want remote notification capability, since users need to be able to call in from any phone in order to log in and listen to messages.

You can either leave it up to users to create their own passwords from the telephone set or create a password for VMUIF users. See "Changing a user's password" on page 9-91.

Adding a local voice user

Introduction

Local voice users are added in the Add a Local Voice User screen. There are a number of things you must do in this screen in order to define a local voice user.

Administration level

Local voice users can only be added from Customer Administration.

Procedure

This is a high-level procedure that lists the steps involved in adding a local voice user. Detailed step-by-step procedures are provided on the following pages.

Step	Action	Page
1	Access the Add Local Voice User screen.	9-9
2	Enter user information such as the user's first and last names.	9-14
3	Assign the user to a class of service.	9-17
4	Specify the following DNs for the user if necessary: • up to seven additional extension DNs • a revert DN • the MWI DN (if different from the mailbox number)	9-21
5	Record a personal verification for the user if necessary. **Note:** Most users record their own verifications.	9-32

Step	Action	Page
6	If remote notification is enabled for the user, create a remote notification schedule if necessary. **Note:** Users can create their own schedules from the telephone set.	9-34
7	Change the following if necessary: • If the interface is MMUI, disable/enable name dialing by external callers (default is enabled). • If Hospitality is installed, set the hospitality user class (default is guest). • If the interface is VMUIF, select the volume level. • If more than one language is installed, select the user's preferred language.	9-37
8	Save the local voice user.	9-41

Accessing the Add Local Voice User screen

Administration level

The Add Local Voice User screen is only accessible from Customer Administration. This is because users must be added to customer groups, and you must, therefore, first select the customer group to which you want to add users.

Mailbox numbers

To access the Add Local Voice User screen, you must enter the user's mailbox number.

Valid range

The mailbox number can be up to 18 digits long. It can be a number between 10 and 999999999999999999.

System addressing length

If the system addressing length is set to a non-zero value, the length of all mailbox numbers must equal the system addressing length.

The system addressing length is defined in the General Options screen for each customer group.

Potential conflicts

Make sure mailbox numbers do not conflict with any of the following numbers:

- the broadcast mailbox number (default is 5555)
- the network broadcast prefix
- other DNs
- the name dialing prefix (default is 11)
- the delivery to non-user prefix
- customer distribution list numbers
- other mailbox numbers
- the AMIS compose prefix (default is 13)
- networking prefixes (if networking is installed)

Before you begin

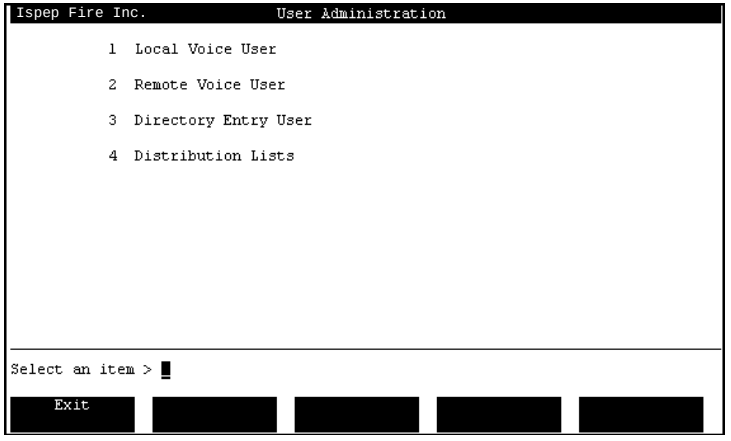
You must first select the customer group to which you want to add local voice users. See "Selecting a customer to view or modify" on page 5-17.

Procedure

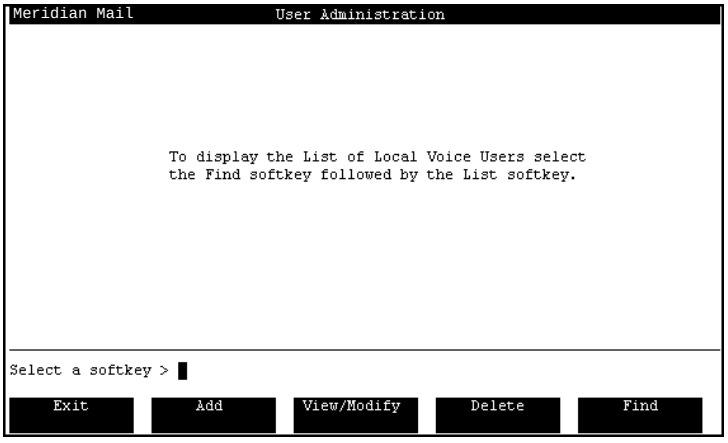
To access the Add Local Voice User screen, follow these steps.

Starting Point: Customer Administration Menu

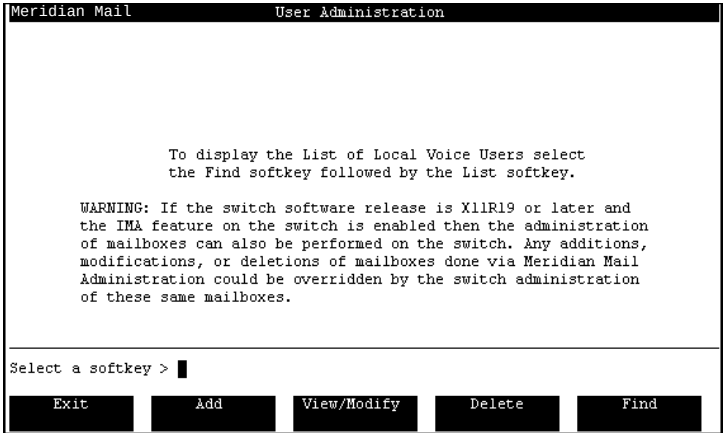
Step	Action
1	Select Local Voice User. **Result:** The User Administration Menu is displayed.



Step	Action
2	Select Local Voice User. **Result:** This screen is displayed if Integrated Mailbox Administration (IMA) is not installed.



This screen is displayed if IMA is installed.


Meridian Mail
User Administration
To display the List of Local Voice Users select
the Find softkey followed by the List softkey.
WARNING: If the switch software release is X11R19 or later and
the IMA feature on the switch is enabled then the administration
of mailboxes can also be performed on the switch. Any additions,
modifications, or deletions of mailboxes done via Meridian Mail
Administration could be overridden by the switch administration
of these same mailboxes.
Select a softkey >
Exit
Add
View/Modify
Delete
Find

3	Press the [Add] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the user's mailbox number and press <Return>. **Result:** The Add Local Voice User screen is displayed. The number you entered is used to fill in the following fields: Mailbox Number, Primary Extension DN, and Message Waiting Indication DN.

The Add Local Voice User screen

Feature-dependent fields

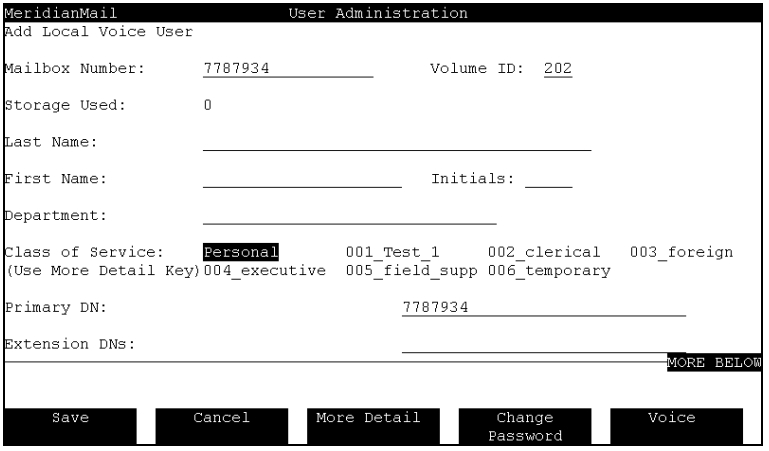
The fields that appear in this screen will vary depending on the following factors:

- When the interface is MMUI, the following fields are displayed (that are not applicable to VMUIF):
  - Department
  - Name Dialable by External Callers
- When the interface is VMUIF, the following field is displayed (that is not applicable to MMUI):
  - Volume level
- If Remote Notification is enabled in the user's class of service, the Remote Notification Schedules field is displayed.
- If Hospitality is installed, the Hospitality User Class field is displayed after the Name Dialable by External Callers field.
- If multiple languages are installed, the Preferred Language field is displayed at the bottom of the screen.

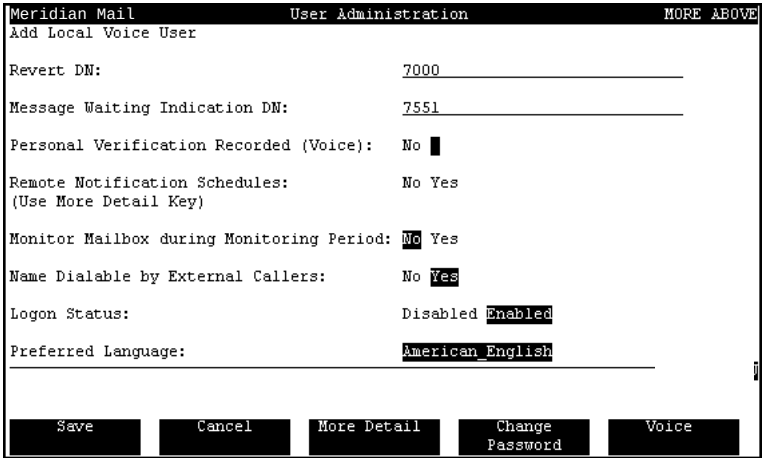
The screen

This is the MMUI version of the Add Local Voice User screen.

Part 1



Part 2



Entering user information

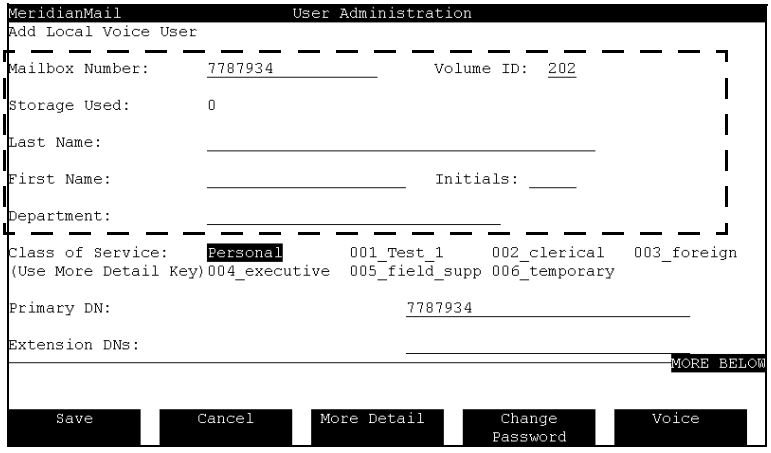
Introduction

The first step in adding a local voice user is to enter information about the user such as the user's first and last names, and the department to which the user belongs.

The Add Local Voice User screen

The dotted box highlights the fields in which you enter user information.

Part 1



Field descriptions

This table describes the fields in which you enter user information.

Mailbox Number	
Description	The user's mailbox number
Default	The number you entered to access the Add Local Voice User screen
Maximum length	18 digits
Valid Range	10 to 999999999999999999
Mandatory	The user cannot be saved if this field is blank.

Volume ID	
Description	This is the hard disk volume to which the local voice user is assigned. This is the volume where user messages and user profiles are stored.
Default	The volume with the greatest amount of free space at the time the [Add] softkey is pressed.

Storage used	
Description	This read-only field indicates how many minutes of voice messages are stored for this user. This number is rounded up to the nearest minute.
VMUIF submailboxes	If submailboxes are enabled, this number also indicates the storage space taken up by all submailbox greetings and voice messages.

Last Name and First Name	
Description	The user's first and last names.
Maximum length	You can enter up to 41 characters for the last name and 21 characters for the first name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).
Attention	Make sure the spelling is correct and use alphanumeric characters only. These fields are used by name dialing and name addressing.

Initials	
Description	Initials can be used to distinguish users with identical first and last names. They are not used by the name dialing and name addressing feature.
Default	Blank If you leave this field blank, Meridian Mail will automatically insert the first initial of the user's first name when you save the user.
Maximum length	5 characters

Department	
Description	The user's department
Interface	MMUI only
Default	This field is blank for the first user you add. For subsequent users, this field defaults to the department entered for the last user you added.
Maximum length	31 characters Make the first 12 characters unique. If you want to later find users based on department, the List of Local Voice Users screen displays only the first 12 characters of the department name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).

Procedure

To enter user information, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Is the current volume the volume to which you want to assign the user? • If yes, go to step 2. • If no, change the volume ID.
2	Enter the user's last name.
3	Enter the user's first name.
4	Enter the user's initials if needed to distinguish this user from another user with the same first and last name.
5	If the interface is MMUI, enter the user's department. **Note:** Make sure that the first 12 characters are unique.
6	Go to page 9-17 to continue defining the user.

Assigning a user to a class of service

Introduction

All local voice users must be assigned to a class of service. The class of service to which a user belongs determines things like the user's voice storage limit, the maximum message length, and the retention period for read messages.

Personal classes of service versus defined classes of service

You should assign most users to one of the classes of service you have already defined in Class of Service Administration. However, there may be some users with special requirements. Instead of defining a class of service for just one user (through Class of Service Administration), create a unique personal class of service here in the Add Local Voice User screen.

To assign a user to a defined class of service, see "Assigning a user to a defined class of service" on page 9-18.

To create a personal class of service for a user, see "Creating a personal class of service" on page 9-19.

Maintenance issues

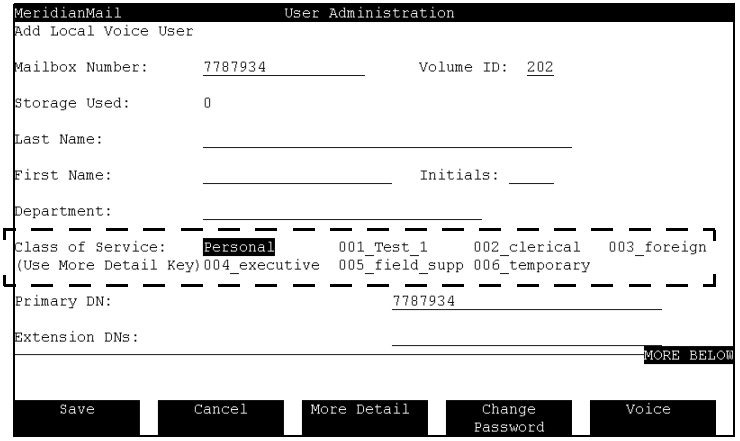
Each personal class of service that you create will have to be maintained separately. You should, therefore, minimize the number of personal classes of service that you create.

Assigning a user to a defined class of service

To assign a user to a class of service that has been defined in Class of Service Administration, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Move your cursor to the Class of Service field, and select the class of service to which you want to assign the user.



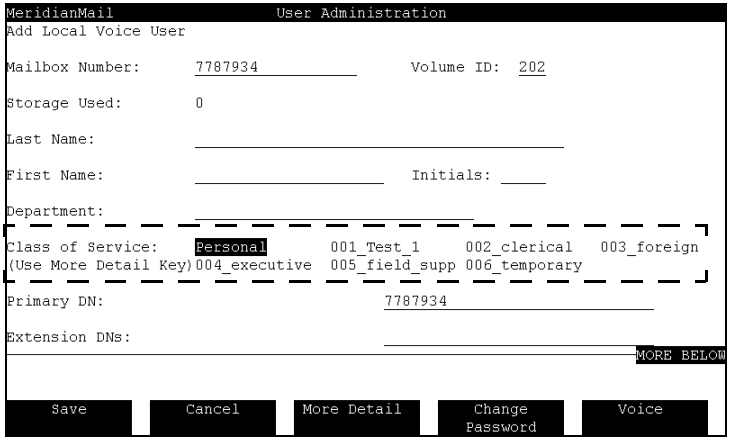
2	Do you want to view the class of service definition to verify that this is an appropriate class of service for this user? • If yes, go to step 3. • If no, go to step 6.
3	Press the [More Detail] softkey. **Result:** The Class of Service definition is displayed. You cannot modify any fields in this screen.
4	Review the class of service configuration to see if it is appropriate for the user.
5	Press the [Return to Basic Fields] softkey to return to the Add Local Voice User screen.
6	Go to page 9-21 to continue defining the local voice user.

Creating a personal class of service

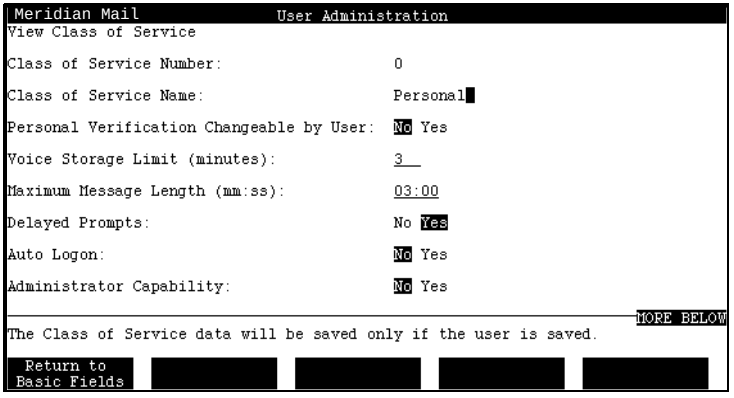
To create a unique personal class of service for a user, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Move your cursor to the Class of Service field, and select Personal.



2	Press the [More Detail] softkey. **Result:** The View Class of Service screen is displayed.


Meridian Mail User Administration
View Class of Service
Class of Service Number: 0
Class of Service Name: Personal
Personal Verification Changeable by User: No Yes
Voice Storage Limit (minutes): 3
Maximum Message Length (mm:ss): 03:00
Delayed Prompts: No Yes
Auto Logon: No Yes
Administrator Capability: No Yes
MORE BELOW
The Class of Service data will be saved only if the user is saved.
Return to Basic Fields

3	Make the necessary modifications. See Chapter 27, “Class of Service administration. ”

Step	Action
4	Press the [Return to Basic Fields] softkey when you are done modifying the class of service. **Result:** The Add Local Voice User screen is displayed. **Note:** The personal class of service will be saved when you save the local voice user.
5	Go to page 9-21 to continue defining the local voice user.

Primary DN and extension DNs

Introduction

The next step in adding a local voice user is to identify and define the extension DNs, including the primary DN, associated with the user.

Definition: extension DNs

An extension DN is a dialable number that, when dialed, rings a telephone.

When telephone set configuration is done in the Meridian 1, one or more DNs are defined for each telephone set. These are the extension DNs that you need to enter in Meridian Mail for each user.

Definition: primary DN

The primary DN is the "main" extension DN. All phones will have a primary DN.

The primary DN field

When you add a mailbox user, the Primary DN field is prefilled with the mailbox number that you entered to access the Add Local Voice User screen.

Call sender

When a user uses the Call Sender feature to call the sender of a message, Call Sender attempts to place the call to the primary DN only.

Note: The Call Sender feature can be supported on a network with CO trunks if

1. the network is configured in the "None" dialing plan
2. the "Dial Prefix" field is properly defined

Extension DNs

In addition to the primary DN, users can have a number of additional DNs programmed on their telephone sets. Meridian Mail supports seven additional extension DNs in addition to the primary DN, for a total of eight supported extension DNs.

Requirements

All DNs defined on a user's telephone set must be defined in Meridian Mail. If a call comes in on a non-primary extension DN which is not defined for the mailbox user, the mailbox will not be found and, as a result, messages cannot be left.

Mailboxes for users without phones

You can create a mailbox (add a local voice user) for people who do not have phones. To do this, make all DN fields blank.

Callers can use thru-dial services and express messaging to leave messages for these users. Users can then call into their mailbox from any phone in order to pick up voice messages.

Entering the extension DNs (primary and non-primary)

See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 9-29.

Duplicating extension DNs

Extension DNs should not duplicate any other DN already registered in Meridian Mail, either as a primary or a secondary DN. Meridian Mail prevents duplications, unless you have changed the "Allow Duplicate User DNs" field setting to Yes in the General Options screen (the default is No).

In the case of a duplication, Meridian Mail will only ring one of the DNs, not both, when the number is dialed.

The revert DN

Introduction

Another type of DN that is associated with each user is the revert DN.

Definition: revert DN

The revert DN is a directory number to which callers or users are transferred under certain specific conditions.

When the revert DN is used

The revert DN is used under two conditions:

Call answering

A caller can press "0" during a call answering session in order to transfer to another number (such as that of an attendant or secretary). This gives callers the chance to transfer to a person for assistance.

Mailbox thru-dial (extension dialing)

Mailbox thru-dial allows MMUI users to dial a number while they are logged in to their mailbox. The user enters "0" followed by the number. If the user waits for more than 2 seconds after entering "0," he or she is transferred to the revert DN.

Revert for MMUI users

For MMUI users, you can specify a customer-wide revert DN. This is done in the Attendant DN field in the General Options screen at the customer administration level. The attendant DN is used if there is no revert DN defined for a user.

Custom revert

The MMUI telephone set interface has a feature called Custom Revert that allows MMUI users to define their own revert DNs. You can either

- allow users to define their own revert DNs

  or

- prohibit users from defining their own DNs and define one customer-wide revert DN for all users in a customer group

In this case, you can define a different revert DN for some users in the Add or View/Modify Local Voice User screen.

Allowing MMUI users to define their own revert DNs

To allow MMUI users to define their own revert DNs through the telephone set, you must ensure that appropriate restrictions are applied to the Custom Revert feature so that users do not enter unauthorized DNs, such as long distance numbers.

To allow users to define their own revert DNs, you must do the following.

1. Define an Attendant DN for each customer group in the General Options screen.

   This will serve as a default or backup for users who do not define a revert DN.

   See “Setting the attendant DN” on page 14-31.

2. Create a restriction/permission list that contains the restriction and permission codes you want to apply to the Custom Revert feature.

   This list cannot have all digits from 0 to 9 as restriction codes (the default). At least some digits have to be permitted to allow users to specify a DN.

   See the section “Restriction/Permission lists” on page 7-89.

3. In the classes of service to which you will be assigning users, select one of the above restriction/permission lists in the Custom Revert Restriction/Permission List field.

   This imposes the proper restrictions on the DNs that users try to define as their custom revert DNs.

   See “The Add Class of Service screen (MMUI)” on page 27-13.

4. Assign users to the appropriate class(es) of service.

5. Leave the Revert DN field blank in the Add Local Voice User screen, or enter the DN if you know where the user wants to revert calls.

Prohibiting MMUI users from defining revert DNs

To prohibit MMUI users from defining their own Revert DNs, you must assign a restriction/permission list that has the digits 0 to 9 as restriction codes to the custom revert feature.

This does not prevent you from defining a Revert DN in User Administration. It only affects telephone set definition of this DN.

To prohibit users from defining their own revert DNs, you must do the following.

1. Define an Attendant DN for each customer group in the General Options screen.

   This will serve as the revert DN for all users in the customer group.

   See “Setting the attendant DN” on page 14-31.
2. Create a restriction/permission list in which the digits 0 to 9 are entered as restriction codes.

   See the section “Restriction/Permission lists” on page 7-89.
3. In the classes of service to which you will be assigning users, select the fully restricted restriction/permission list in the Custom Revert Restriction/Permission List field.

   See “The Add Class of Service screen (MMUI)” on page 27-13.
4. Assign users to the class of service.
5. Leave the Revert DN field blank in the Add Local Voice User screen if the Attendant DN is appropriate for the user; or, enter a different revert DN for the user.

Revert for VMUIF users

You cannot configure an Attendant DN for VMUIF customers. This means that if no Revert DN is defined for a VMUIF user, callers will not be able to press “0” to transfer to another DN.

For most VMUIF users, this is desirable. However, if revert capability is required for a user, you must define a Revert DN in the Add Local Voice User screen.

Entering the revert DN

See “Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN” on page 9-29.

The message waiting indication DN

Introduction

The next DN that is associated with a local voice user is the message waiting indication (MWI) DN.

Description

This is the DN to which the message waiting indication (flashing light or stutter dial tone) is sent

- when the user has a new voice message waiting to be read
- in a hospitality system, to notify the user of an external message

  An external message can be a written message that has been taken by the front desk, in which case the front desk clerk can turn a guest's MWI on in order to notify the guest of the message. The MWI can also be used to indicate that there is a message waiting that can be accessed through the hotel's TV messaging system.
- from an ACCESS application to indicate that a certain type of message has been received for the user (The message type depends on the ACCESS application.)

The default MWI DN

When you add a local voice user, this DN is automatically set to the number you entered as the mailbox number to access the Add Local Voice User screen. Typically, you leave this DN as it is so that it is the same as the mailbox number and primary DN. This is because you usually want the indication to go to the user's phone where the user will see the indication.

Choosing another MWI DN

However, there are a number of cases where the MWI DN should be configured as something other than the user's primary DN. These conditions are outlined in this table.

IF	THEN
the user wants the indication to go to another phone, such as a secretary's	enter the other person's primary DN as the MWI DN.
the user has a mailbox only, but no physical phone	make the MWI DN field blank.

Example

A senior executive has requested that her secretary be notified of her new voice messages so that the secretary can screen them. In the executive's mailbox setup, you enter the secretary's primary DN as the MWI DN. However, this is also the secretary's MWI DN. This means that the secretary will not be able to tell who new messages are for. The secretary will have to log on to both mailboxes to find out.

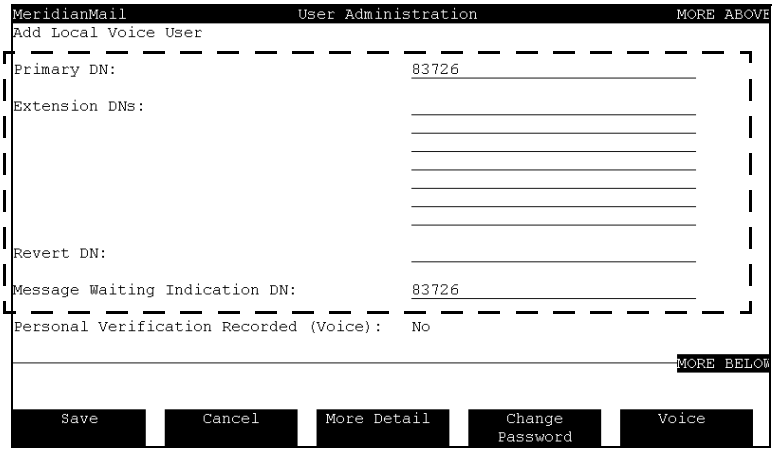
Entering the MWI DN

See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 9-29.

Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN

DN fields in the Add Local Voice User screen

The dotted box highlights the fields that are used to define user DNs.



Field descriptions

This table describes the fields you use to define DNs that are associated with a user.

Primary DN	
Description	When dialed, this number rings a user's telephone. It is the number used for Call Sender and Name Dialing.
Maximum length	30 digits
Default	This field is filled in with the mailbox number you entered to access the Add Local Voice User screen.
More information	See "Primary DN and extension DNs" on page 9-21.

Extension DNs	
Description	These fields allow seven secondary DNs to be entered. This means that a caller can dial any one of these numbers and reach the user.
Maximum length	30 digits
Default	Blank
More information	See “Primary DN and extension DNs” on page 9-21.

Revert DN	
Description	This is the DN to which calls are transferred when • a caller presses “0” during a call answering session • an MMUI user trying to use mailbox thru-dial waits more than 2 seconds after dialing the “0”
Maximum length	30 digits
Default	Blank
More information	See “The revert DN” on page 9-23.

Message Waiting Indication DN	
Description	This is the DN to which message waiting indications are sent when the user has unread voice messages, external HVS messages, or messages from an ACCESS application. This DN is usually the same as the user’s primary DN.
Conditions of display	This field is displayed if the Message Waiting Indication Options field in the user’s Class of Service is set to something other than None.
Default	The mailbox number you entered to access the Add Local Voice User screen
More information	See “The message waiting indication DN” on page 9-27.

Procedure

To specify DNs for the user, follow these steps.

Starting Point: The Local Voice User screen

Step	Action
1	Does the user have a phone? • If yes, go to step 2. • If no, make all DN fields blank, and go to step 4.
2	Does the user have more than one DN? • If yes, go to step 3. • If no, go to step 4.
3	Enter the user's other DN(s) in the Extension DN fields. **Note:** For details, see "Primary DN and extension DNs" on page 9-21.
4	Enter a Revert DN if necessary. **Note:** For details, see "The revert DN" on page 9-23.
5	Change the Message Waiting Indication DN if necessary.

IF	THEN
the user should be notified of new messages at his or her phone	leave the default MWI DN (same as mailbox number).
the user does not have a phone	delete the MWI DN.
the user wants someone else to be notified of his or her messages	enter that person's DN in the MWI DN field.

Note: For more information, see "See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 9-29." on page 9-26.

6 Continue defining the local voice user.

IF you want to	THEN go to
record a personal verification for the user	page 9-32.
create a remote notification schedule for the user	page 9-34.
define other local voice user characteristics	page 9-37.

Recording a personal verification for a user

Introduction

Ideally, users should record personal verifications in their own voice. However, as administrator, you can record personal verifications from the administration terminal on behalf of users.

When to use

If the user belongs to a class of service in which the Personal Verification Changeable by User field is set to No and the user needs a personal verification, you will have to record it for him or her.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey.
3	Enter the extension of the phone you will use to record the verification, and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.
5	Press the [Record] softkey.
6	At the sound of the beep, speak the user's name (and, optionally, the user's extension). **Example:** *"Heather McGee at extension 8523."*
7	Press the [Stop] key to stop recording.
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.

Step	Action
9	Do you want to rerecord the verification? • If yes, repeat steps 5 to 8. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.
11	Continue defining the local voice user.

IF you want to	THEN go to
create a remote notification schedule for the user	page 9-34.
define other local voice user characteristics	page 9-37.

Creating a remote notification schedule for a user

Introduction

The Remote Notification Schedules field is displayed if

- Outcalling is installed
- the Remote Notification Capability field in the user's class of service is set to Yes

User-defined versus administrator-defined

Users can create their own remote notification schedules from their telephone sets. You may, however, have to create remote notification schedules for users under the following conditions:

- The Remote Notification Keypad Interface field in the user's class of service is set to No, and the user cannot create his or her own schedule from the telephone set.
- A user does not want to use the telephone set interface to create a schedule and asks you to create it for him or her.
- New features in Meridian Mail 12 (concerning the type of remote notification a user receives) cannot be accessed through the telephone keypad interface, and your user requires them.

See also

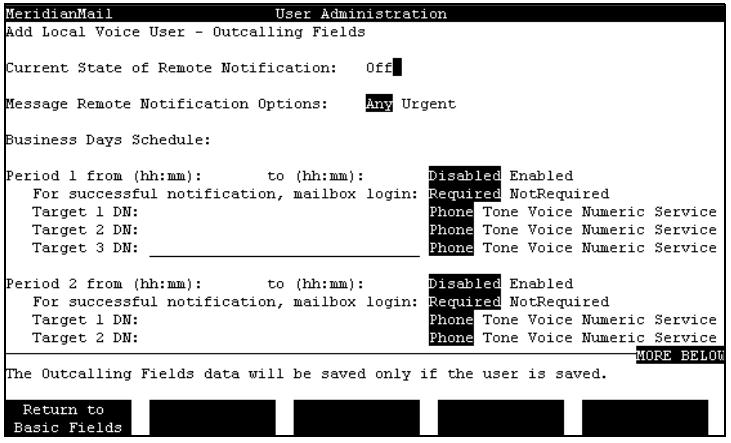
For more information about remote notification schedules, refer to the *Outcalling Guide* (NTP 555-7001-320).

Procedure

To create a remote notification schedule for a user, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Put your cursor on the Remote Notification Schedules field and press the [More Detail] softkey. **Note:** The Outcalling fields are displayed.


MeridianMail User Administration
Add Local Voice User - Outcalling Fields
Current State of Remote Notification: Off
Message Remote Notification Options: Any Urgent
Business Days Schedule:
Period 1 from (hh:mm): to (hh:mm): Disabled Enabled
For successful notification, mailbox login: Required NotRequired
Target 1 DN: Phone Tone Voice Numeric Service
Target 2 DN: Phone Tone Voice Numeric Service
Target 3 DN: Phone Tone Voice Numeric Service
Period 2 from (hh:mm): to (hh:mm): Disabled Enabled
For successful notification, mailbox login: Required NotRequired
Target 1 DN: Phone Tone Voice Numeric Service
Target 2 DN: Phone Tone Voice Numeric Service
MORE BELOW
The Outcalling Fields data will be saved only if the user is saved.
Return to Basic Fields

2	Create a business day schedule. For each required time period a. Enter the from and to time. b. Select Enabled to enable the time period. c. Specify whether the user must log into their mailbox for Meridian Mail to consider the notification “successful” and stop its notification attempts. d. Enter up to three target DNs. e. For each target DN, specify the type of device. For pagers, specify the Pager Callback Number. For general access pager services, enter the Pager ID Number.
3	Create a nonbusiness days schedule. For each required time period, repeat steps 2a. to 2d.
4	Do you need to create a temporary schedule? • If yes, repeat steps 2a. to 2d. for each required time period. • If no, go to step 5.

Step	Action
5	Press the [Return to Basic Fields] softkey to return to the basic fields in the Add Local Voice User screen.
6	Go to page 9-37 to continue defining the local voice user.

Setting other local voice user characteristics

Introduction

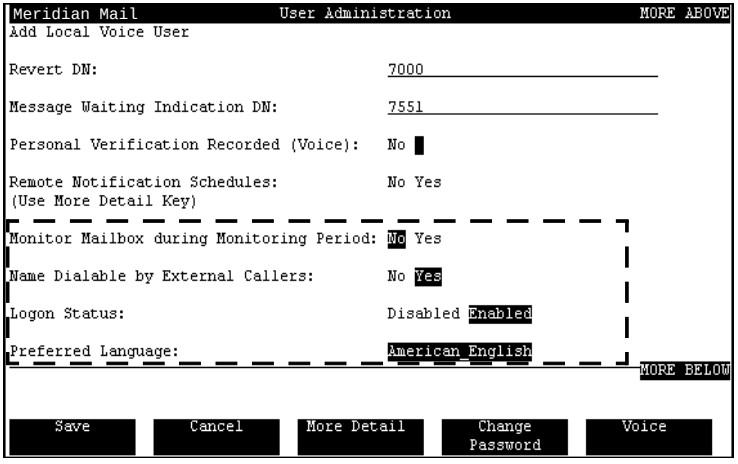
To finish defining a local voice user, you may have to modify some or all of the remaining fields:

- Monitor Mailbox during Monitoring Period
- Name Dialable by External Callers (MMUI only)
- Hospitality User Class (if Hospitality is installed and used by the customer)

  Only one customer can be set up with hospitality on a multi-customer system. Once a customer is added with the Hospitality interface, it will always have hospitality.
- Volume Level (VMUIF only)
- Preferred Language (if multiple languages are installed)

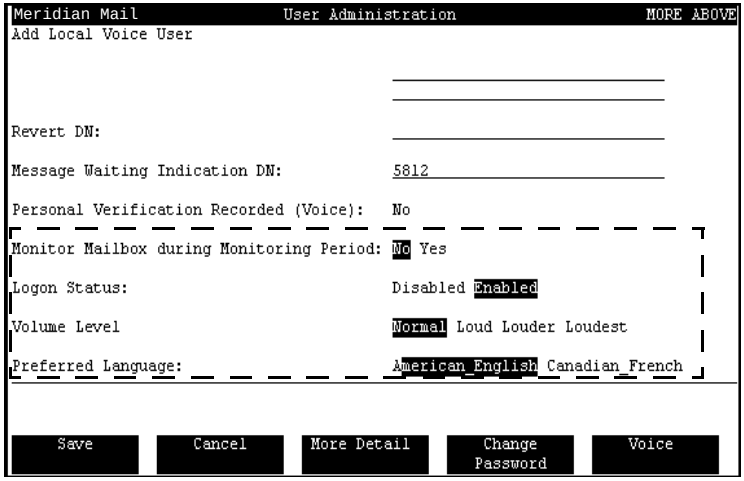
Relevant fields: MMUI

The dotted box highlights the fields that are available when the interface is MMUI.



Relevant fields: VMUIF

The dotted box highlights the fields that are available when the interface is VMUIF.



Field descriptions

This table describes the fields that are used to define the remaining local voice user characteristics.

Monitor Mailbox during Monitoring Period	
Description	This field determines whether the mailbox is monitored for logons. This is a security feature that you can use when you suspect a hacker is trying to get into a particular mailbox. Typically, you would not enable this feature for new users, but only for existing users when hacker activity is suspected.
Interface	MMUI and VMUIF
Default	No
More information	See “Monitoring mailbox logins for suspected hacker activity” on page 9-92.

Name Dialable by External Callers	
Description	This field determines whether external callers can use name dialing to call the user. For users that have their calls screened, you might want to disable this feature. Otherwise, any caller can get through to the user's extension through a thru-dialer by entering their name.
Interface	MMUI
Default	Yes
Valid Options	Yes, No

Hospitality User Class	
Description	This field indicates whether the mailbox belongs to a staff member or guest.
Feature dependencies	This field is displayed only if Hospitality is installed and enabled for the customer group.
Default	Guest
Valid Options	Guest, Staff

Volume Level	
Description	This is the volume level at which recorded prompts and voice messages are played.
Interface	VMUIF
Default	Normal
Valid Options	Normal, Loud, Louder, Loudest

Preferred Language	
Description	This is the language in which prompts are played to the user during a login session and to callers during call answering and express messaging.
Feature dependencies	This field is displayed only if more than one language is installed on the system.
System override	If the Default Language Overrides User's Preferred Language field in the Voice Messaging Options screen is set to Yes, call answering and express messaging prompts will be played to callers in the system default language. Prompts to the user while logged in to Meridian Mail continue to be played in the user's preferred language.
Default	The first language in the list
More information	See "The default language and the user's preferred language" on page 21-13.

Procedure

To set the remaining local voice user characteristics, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	If this is an MMUI customer group, do you want to prohibit external callers from using name dialing to call this user? • If yes, set the Name Dialable by External Callers field to No. • If no, leave the Name Dialable by External Callers field set to Yes.
2	If Hospitality is installed, are you adding a mailbox for a guest? • If yes, leave the Hospitality User Class as “Guest.” • If no, set the Hospitality User Class field to “Staff.”
3	If this is a VMUIF customer group, change the volume level if necessary.
4	If more than one language is installed on the system, specify the user’s preferred language.
5	Do you want to save the local voice user as currently defined? • If yes, press the [Save] softkey. **Note:** If the entered DN is already in use by another Local Voice User or Remote Voice User, a warning message will appear. You can either modify the DN or press the [Save] softkey to save the DN for the user who originally had the DN. • If no, make any necessary changes and then press [Save], or press [Cancel] if you do not want to add this user.

Section B: Finding local voice users

In this section

Overview	9-44
Wildcard characters	9-45
Accessing the Find Local Voice Users screen	9-47
The Find Local Voice Users screen	9-48
Restrictions on how you can combine search criteria	9-65
Finding, listing, and printing local voice users	9-67
Reassigning a subset of local voice users to another class of service	9-71

Overview

Introduction

The Find function allows you to find a single local voice user or a subset of local voice users that meet the search criteria that you specify in the Find Local Voice User screen.

Administration level

The Find function works only within a single customer group. It cannot find users throughout the entire Meridian Mail system.

Examples of use

Here are some examples of how you can use the Find function. You can

- find Pierre LaMontaigne's user profile when you do not know his mailbox number
- find all users who belong to Class of Service 12 and reassign them to Class of Service 9
- find all users who are in the Marketing department that do not have Remote Notification capability, and reassign them to a class of service in which Remote Notification is enabled
- find all users who have exceeded their voice storage limit
- find all users whose primary DN differs from their MWI DN
- find all users in the Customer Documentation department, which has been renamed the Information Products department, so that you can update their department definitions
- find all users whose mailboxes are disabled (due to too many invalid logon attempts)
- find all users who have a specific voice storage limit so that you can either increase or decrease this limit
- find all users whose passwords have expired
- find all users on a particular volume (which is overloaded) so that you can move some of them to another volume

Wildcard characters

Definition: wildcard

A wildcard is a character that is used in a search string to represent an unknown or variable character or string of characters.

Purpose

Wildcards have two main purposes. They allow you to find

- a particular user when you do not know the user's mailbox number and have only partial information about the user
- a range of users

Types of wildcards

There are two wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.

Where you can use wildcards

You can enter wildcards in the following fields:

- Mailbox Number
- Last Name
- First Name
- Department
- Extension Number (DN)
- Message Waiting Indication DN

Examples

The following examples show how wildcards can be used to find a range of users.

You enter	Result
"210_" in the Mailbox Number field	All mailboxes in the range 2100 to 2109 are found.
"7_99" in the Extension Number field	Users with the following extension DNs are found: 7099, 7199, 7299, 7399, 7499, 7599, 7699, 7799, 7899, and 7999.
"3+" in the Mailbox Number field	All mailboxes beginning with 3 are found.
"+Engineering" in the Department field	Users belonging to all engineering departments are found (such as Software Engineering, Hardware Engineering, and Information Engineering).

Accessing the Find Local Voice Users screen

Administration level

The Find Local Voice Users screen is only accessible from Customer Administration. This is because users belong to customer groups, and you must, therefore, first select the customer group to which the user(s) who you want to find belong.

Procedure

To access the Find Local Voice Users screen, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [Find] softkey. **Result:** The Find Local Voice Users screen is displayed.

The Find Local Voice Users screen

Introduction

The fields in the Find Local Voice Users screen vary depending on the interface (MMUI or VMUIF).

The screen: MMUI version

This is how the Find Local Voice Users screen looks when the interface is MMUI.

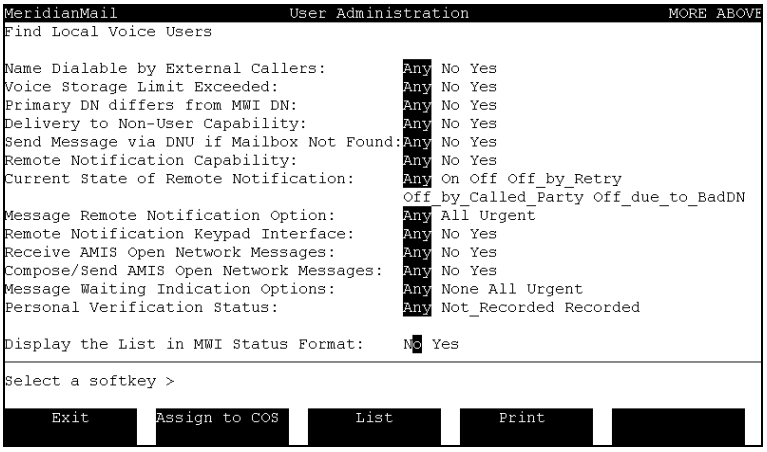
Part 1

```
MeridianMail                User Administration
Find Local Voice Users

Status:          Any Enabled Disabled Expired Violation
Mailbox Number:  ____________________              Volume ID: ___  COS: ___
Last Name:       ____________________________________________
First Name:      ____________________
Department:      ____________________________________
Extension Number (DN):                    ____________________________________
Message Waiting Indication DN:            ____________________________________
Revert DN:                                ____________________________________
Voice Storage Limit (minutes):            ____
Read Message Retention (days):            __
Minimum Number of Invalid Logon Attempts: __
Minimum Number of Days since Last Logon:  __
Minimum Number of Days since Pswd Changed:__
Maximum Message Length (mm:ss):           _____
Maximum CA Message Length (mm:ss):        _____
Receive Composed Messages:                Any No Yes
                                                                    MORE BELOW
Select a softkey >

 Exit | Assign to COS | List | Print |
```

Part 2

```
MeridianMail                User Administration                     MORE ABOVE
Find Local Voice Users

Auto Logon:                                 Any No Yes
Broadcast Capability:                       Any No Yes
Administrator Capability:                   Any No Yes
Internal Personal Greeting Recorded:        Any No Yes
External Personal Greeting Recorded:        Any No Yes
Temporary Absence Greeting Recorded:        Any No Yes
Auto Deletion of Invalid PDL Addresses:     Any No Yes
Personal Verification Changeable by User:   Any No Yes
Name Dialable by External Callers:          Any No Yes
Voice Storage Limit Exceeded:               Any No Yes
Primary DN differs from MWI DN:             Any No Yes
Delivery to Non-User Capability:            Any No Yes
Send Message via DNU if Mailbox Not Found:  Any No Yes
Remote Notification Capability:             Any No Yes
Current State of Remote Notification:       Any On Off Off_by_Retry
                                            Off_by_Called_Party Off_due_to_BadDN
                                                                    MORE BELOW
Select a softkey >

 Exit | Assign to COS | List | Print |
```

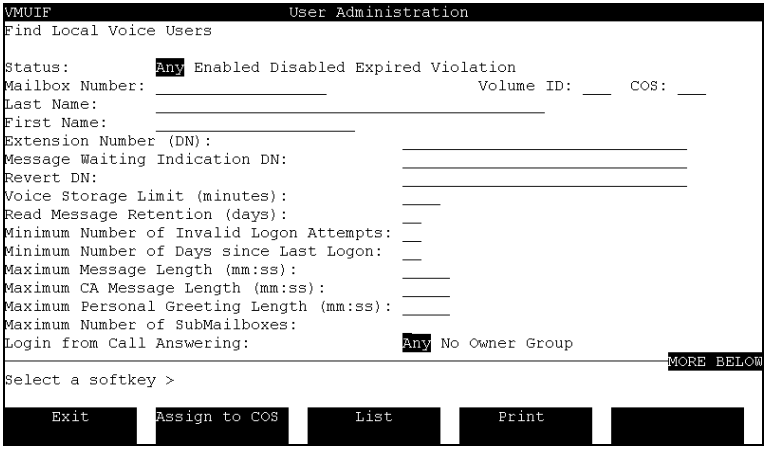
Part 3


MeridianMail User Administration MORE ABOVE
Find Local Voice Users
Name Dialable by External Callers: Any No Yes
Voice Storage Limit Exceeded: Any No Yes
Primary DN differs from MWI DN: Any No Yes
Delivery to Non-User Capability: Any No Yes
Send Message via DNU if Mailbox Not Found: Any No Yes
Remote Notification Capability: Any No Yes
Current State of Remote Notification: Any On Off Off_by_Retry
Off_by_Called_Party Off_due_to_BadDN
Message Remote Notification Option: Any All Urgent
Remote Notification Keypad Interface: Any No Yes
Receive AMIS Open Network Messages: Any No Yes
Compose/Send AMIS Open Network Messages: Any No Yes
Message Waiting Indication Options: Any None All Urgent
Personal Verification Status: Any Not_Recorded Recorded
Display the List in MWI Status Format: No Yes
Select a softkey >
Exit
Assign to COS
List
Print

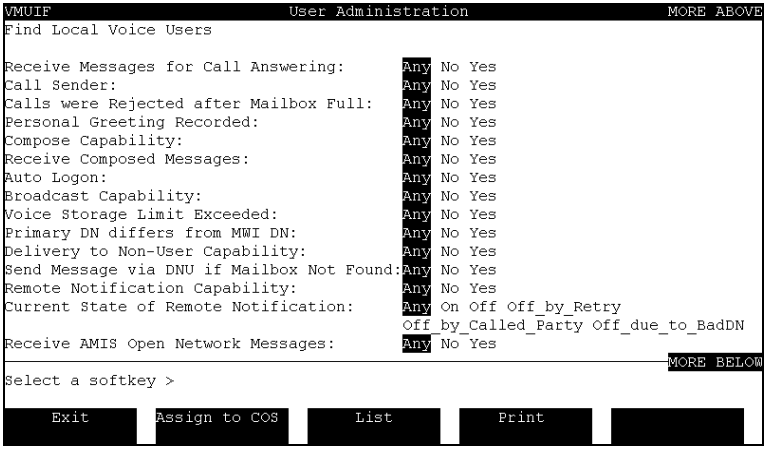
The screen: VMUIF version

This is how the Find Local Voice Users screen looks when the interface is VMUIF.

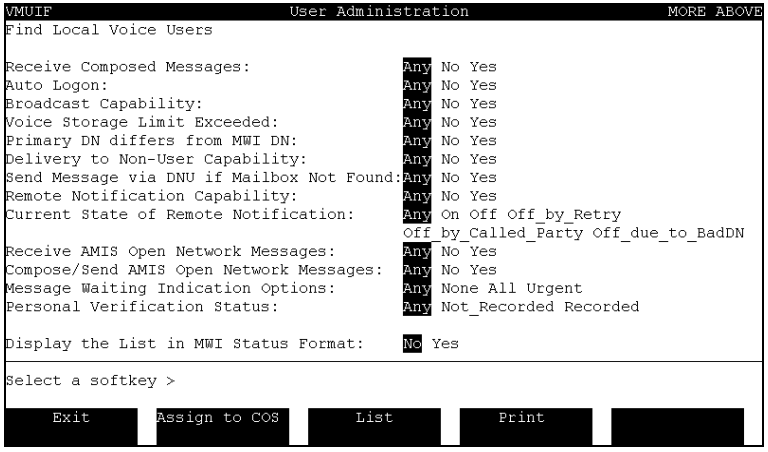
Part 1



Part 2


VMUIF User Administration MORE ABOVE
Find Local Voice Users
Receive Messages for Call Answering: Any No Yes
Call Sender: Any No Yes
Calls were Rejected after Mailbox Full: Any No Yes
Personal Greeting Recorded: Any No Yes
Compose Capability: Any No Yes
Receive Composed Messages: Any No Yes
Auto Logon: Any No Yes
Broadcast Capability: Any No Yes
Voice Storage Limit Exceeded: Any No Yes
Primary DN differs from MWI DN: Any No Yes
Delivery to Non-User Capability: Any No Yes
Send Message via DNU if Mailbox Not Found: Any No Yes
Remote Notification Capability: Any No Yes
Current State of Remote Notification: Any On Off Off_by_Retry
Off_by_Called_Party Off_due_to_BadDN
Receive AMIS Open Network Messages: Any No Yes
MORE BELOW
Select a softkey >
Exit
Assign to COS
List
Print

Part 3


VMUIF User Administration MORE ABOVE
Find Local Voice Users
Receive Composed Messages: Any No Yes
Auto Logon: Any No Yes
Broadcast Capability: Any No Yes
Voice Storage Limit Exceeded: Any No Yes
Primary DN differs from MWI DN: Any No Yes
Delivery to Non-User Capability: Any No Yes
Send Message via DNU if Mailbox Not Found: Any No Yes
Remote Notification Capability: Any No Yes
Current State of Remote Notification: Any On Off Off_by_Retry
Off_by_Called_Party Off_due_to_BadDN
Receive AMIS Open Network Messages: Any No Yes
Compose/Send AMIS Open Network Messages: Any No Yes
Message Waiting Indication Options: Any None All Urgent
Personal Verification Status: Any Not_Recorded Recorded
Display the List in MWI Status Format: No Yes
Select a softkey >
Exit
Assign to COS
List
Print

Field descriptions

These are the fields in the Find Local Voice Users screen that you can fill in to specify your search criteria.

Status	
Description	Use this field to find users with a particular mailbox status.
Default	Any
Valid Options	Any, Enabled, Disabled, Expired, Violation • *Any* finds all users. • *Enabled* finds all users whose mailboxes are enabled. • *Disabled* finds all users whose mailboxes have been disabled from the MMI or due to too many invalid logon attempts per mailbox. This maximum logon attempts value is defined in the Voice Security Options screen. • *Expired* finds all users whose passwords have expired. • *Violation* finds all users whose maximum number of invalid logon attempts per session has been reached or exceeded. This maximum is defined in the Voice Security Options screen.

Mailbox Number	
Description	Use this field to find users within a certain range of consecutive mailbox numbers. This requires the use of wildcards.
Maximum Length	You can enter up to 18 characters.

Volume ID	
Description	Use this field to find all users on a particular volume.
Default	Blank
Valid Options	Any valid user volume

COS	
Description	Use this field to find all users who are assigned to a particular class of service.
Default	Blank
Valid Options	Any class of service that has been created and assigned to the customer group
See Also	If you enter a number in this field, you cannot use any of the fields which concern COS-controlled features. See "Restrictions on how you can combine search criteria" on page 9-65.

Last Name	
Description	Use this field if you want to find a particular user. Use wildcards if you are unsure of the exact spelling.
Default	Blank

First Name	
Description	Use this field if you want to find a particular user. Use wildcards if you are unsure of the spelling.
Default	Blank

Department	
Description	Use this field to find users who belong to a particular department. Use wildcard characters if you are unsure of the exact name or spelling, or if you want to find users in a number of similarly named departments.
Interface	MMUI only
Default	Blank

Extension Number (DN)	
Description	Use this field if you want to find users with a particular primary extension DN. Use wildcards to find users within a range of DNs.
Default	Blank

Message Waiting Indication DN	
Description	Use this field if you want to find users with a particular message waiting indication DN.
Default	Blank

Revert DN	
Description	Use this field to find users who have a specific Revert DN.
Default	Blank
Maximum Length	You can enter a DN up to 30 digits in length.

Voice Storage Limit (minutes)	
Description	Use this field to find users that have a specific voice storage limit.
Default	Blank
Valid Range	1 to 360

Read Message Retention (days)	
Description	Use this field to find users who have their messages automatically deleted after a specified number of days. ***Note:*** The number of days that a message is stored may be set in either the Maximum Read Message Retention field of the customer's Voice Messaging Options or in the Read Message Retention field in the user's Class of Service. When searching with this parameter, the smaller of the two values is used.
Default	Blank
Valid Range	0 to 99

Minimum Number of Invalid Logon Attempts	
Description	Use this field to find users who have at least the specified number of invalid logon attempts. This field is useful for monitoring possible attempts at unauthorized logon.
Default	Blank
Valid Range	0 to 99

Minimum Number of Days since Last Logon	
Description	Use this field to find users who have not logged into their mailbox in at least the specified number of days.
Default	Blank
Valid Range	0 to 99

Minimum Number of Days since Pswd Changed	
Description	Use this field to find users who have not changed their mailbox logon password in at least the specified number of days.
Interface	MMUI only
Default	Blank
Valid Range	0 to 99

Maximum Message Length (mm:ss)	
Description	Use this field to find users who have a specific maximum allowable message length. This is for composed voice messages.
Default	Blank
Valid Range	00:30 to 99:00 in 10-second increments

Maximum CA Message Length (mm:ss)	
Description	Use this field to find users who have a specific maximum allowable call answering message length. These are messages left by callers.
Default	Blank
Valid Range	00:30 to 99:00 in 10-second increments

Maximum Personal Greeting Length (mm:ss)	
Description	Use this field to find users who have a specific maximum personal greeting length.
Interface	VMUIF only
Default	Blank
Valid Range	00:30 to 05:00 in 10-second increments

Maximum Number of SubMailboxes	
Description	Use this field to find users who have a specific maximum number of submailboxes.
Interface	VMUIF only
Default	Blank
Valid Range	0 to 8

Login from Call Answering	
Description	Use this field to find users who are allowed, or not allowed, to log in to their own mailbox while in a call answering session.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Owner, Group • *Any* finds all users. • *No* finds users who are not allowed to log in to their mailbox during a call answering session. • *Owner* finds users who are allowed to log in only if they are connected to their own mailbox. • *Group* finds users who are allowed to log in only if they are connected to a mailbox that belongs to the same customer group.

Receive Messages for Call Answering	
Description	Use this field to find users who are allowed, or not allowed, to receive call answering messages.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Call Sender	
Description	Use this field to find users who have, or do not have, the capability to call the sender of a message.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Calls were Rejected after Mailbox Full	
Description	Use this field to find users who have, or have not had, calls rejected because their mailbox is full.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, a personal greeting recorded.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Compose Capability	
Description	Use this field to find users who are allowed, or not allowed, to compose messages.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Receive Composed Messages	
Description	Use this field to find users who are allowed, or not allowed, to receive composed messages.
Default	Any
Valid Options	Any, No, Yes

Auto Logon	
Description	Use this field to find users who are allowed, or not allowed, to log in to their mailbox without entering a mailbox number or password.
Default	Any
Valid Options	Any, No, Yes

Broadcast Capability	
Description	Use this field to find users who have, or do not have, broadcast capability.
Default	Any
Valid Options	Any, No, Yes

Network Broadcast Capability	
Description	Use this field to find users who have, or do not have, network broadcast capability. ***Note:*** This field is displayed only if the Networking feature is installed and enabled for the customer.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Administrator Capability	
Description	Use this field to find users who have, or do not have, administrator capability.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Internal Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, an internal personal greeting recorded.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

External Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, an external personal greeting recorded.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Temporary Absence Greeting Recorded	
Description	Use this field to find users who have, or do not have, a temporary absence greeting recorded. ***Note:*** If the Temporary Absence Greeting expiry date has passed, then the corresponding mailbox field will be reset to No when the user logs in to their mailbox.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Auto Deletion of Invalid PDL Addresses	
Description	Use this field to find users who have, or do not have, mailboxes with the capability to automatically delete invalid addresses from personal distribution lists.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Personal Verification Changeable by User	
Description	Use this field to find users who have, or do not have, the capability to change their personal verification.
Interface	MMUI only
Default	Any
Valid Options	Any, No , Yes

Name Dialable by External Callers	
Description	Use this field to find users who can, or cannot, be name dialed by external callers.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Voice Storage Limit Exceeded	
Description	Use this field to find users who have, or have not, exceeded their voice storage limit.
Default	Any
Valid Options	Any, No, Yes

Primary DN differs from MWI DN	
Description	Use this field to find users whose primary DN and MWI DN are different or identical.
Default	Any
Valid Options	Any, No, Yes

Delivery to Non-User Capability	
Description	Use this field to find users who have, or do not have, delivery to nonuser capability.
Feature dependencies	This field is displayed only if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Send Message via DNU if Mailbox Not Found	
Description	Use this field to find users who have, or do not have, implicit DNU capability.
Feature dependencies	This field is displayed if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Remote Notification Capability	
Description	Use this field to find users who have, or do not have, remote notification capability.
Feature dependencies	This field is displayed if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Current State of Remote Notification	
Description	Use this field to find users according to their current state of remote notification.
Default	Any
Feature dependencies	This field is displayed if Outcalling is installed.
Valid Options	Any, On, Off, Off_by_Retry, Off_by_Called_Party, Off_due_to_BadDN • *Any* finds all users. • *On* finds all users whose current remote notification state is on. • *Off* finds all users whose current remote notification state is off. • *Off_by_Retry* finds all users whose remote notification state has been turned off after reaching the maximum number of retries. • *Off_by_Called_Party* finds all users whose remote notification state has been turned off by the called party. • *Off_due_to_BadDN* finds all users whose remote notification state has been turned off because a nonfunctional DN was called.

Message Remote Notification Option	
Description	Use this field to find users who are notified when a message is deposited in their mailbox.
Feature dependencies	This field is displayed if Outcalling is installed.
Interface	MMUI only
Default	Any
Valid Options	Any, All, Urgent • *Any* finds all users. • *All* finds all users who are notified when any message is deposited in their mailbox. • *Urgent* finds all users who are notified only when a message marked as Urgent is deposited in their mailbox.

Remote Notification Keypad Interface	
Description	Use this field to find users who have, or do not have, the capability to set up their own remote notification schedules.
Feature dependencies	This field is displayed if Outcalling is installed.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Receive AMIS Open Network Messages	
Description	Use this field to find users who are allowed, or not allowed, to receive AMIS open network messages.
Feature dependencies	This field is displayed if AMIS is installed.
Default	Any
Valid Options	Any, No, Yes

Compose/Send AMIS Open Network Messages	
Description	Use this field to find users who are allowed, or not allowed, to compose and send AMIS open network messages.
Feature dependencies	This field is displayed only if AMIS networking is installed.
Default	Any
Valid Options	Any, No, Yes

Preferred Language	
Description	Use this field to find users who have a specific preferred language.
Feature dependencies	This field is displayed only if more than one language is installed.
Default	Any
Valid Options	Any one of the listed installed languages

Message Waiting Indication Options	
Description	Use this field to find users by when they receive their message waiting indication for new messages, depending on priority.
Default	Any
Valid Options	Any, None, All, Urgent • *Any* finds all users. • *None* finds all users who do not receive a message waiting indication. • *All* finds all users who receive a message waiting indication for any message. • *Urgent* finds all users who receive a message waiting indication only for messages marked as Urgent.

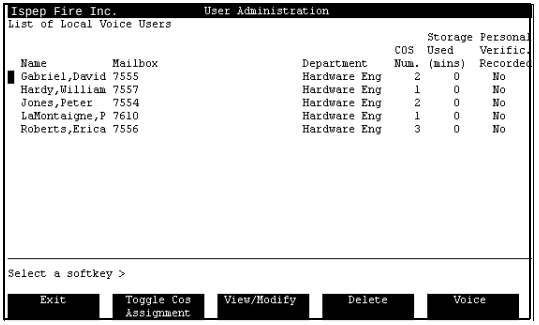
Personal Verification Status

Description	Use this field to find users who do not have, or have, a recorded personal verification.
Default	Any
Valid Options	Any, Not Recorded, Recorded

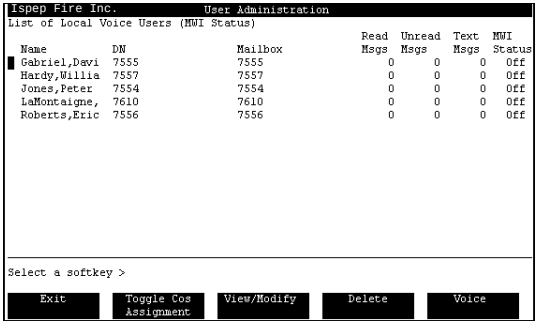
Display the List in MWI Status Format

Description	Use this field to select the format in which you want the list of found users to be displayed or printed. Your selection determines the kind of information that is displayed for each found user.
Default	No
Valid Options	No, Yes

- ***No*** displays the list in General format.


Ispep Fire Inc. User Administration
List of Local Voice Users
Name Mailbox Department COS Num. Storage Used (mins) Personal Verific. Recorded
Gabriel,David 7555 Hardware Eng 2 0 No
Hardy,William 7557 Hardware Eng 1 0 No
Jones,Peter 7554 Hardware Eng 2 0 No
LaMontaigne,P 7610 Hardware Eng 1 0 No
Roberts,Erica 7556 Hardware Eng 3 0 No
Select a softkey >
Exit
Toggle Cos Assignment
View/Modify
Delete
Voice

- ***Yes*** displays the list in MWI Status format.


Ispep Fire Inc. User Administration
List of Local Voice Users (MWI Status)
Name DN Mailbox Read Msgs Unread Msgs Text Msgs MWI Status
Gabriel,Davi 7555 7555 0 0 0 Off
Hardy,Willia 7557 7557 0 0 0 Off
Jones,Peter 7554 7554 0 0 0 Off
LaMontaigne, 7610 7610 0 0 0 Off
Roberts,Eric 7556 7556 0 0 0 Off
Select a softkey >
Exit
Toggle Cos Assignment
View/Modify
Delete
Voice

Restrictions on how you can combine search criteria

Restriction

If you enter a Class of Service number in the COS field, you cannot use any of the class of service feature fields that appear in the Find Local Voice Users screen. If you do so, a message notifies you that this type of search is not allowed.

Rationale

This prevents you from entering self-contradictory combinations that would result in no users being found.

Example

If you enter 12 in the COS field and set DNU Capability to Yes, but DNU is disabled in that class of service, you have a conflict which results in no users being retrieved.

Class of Service fields in the Find screen

The following fields in the Find Local Voice User screen are class of service fields and, therefore, cannot be used in combination with the COS field:

- Voice Storage Limit
- Read Message Retention Time
- Maximum Message Length
- Maximum Call Answering Message Length
- Maximum Personal Greeting Length (VMUIF only)
- Maximum Number of SubMailboxes (VMUIF only)
- Login from Call Answering (VMUIF only)
- Receive Messages for Call Answering (VMUIF only)
- Call Sender (VMUIF only)
- Compose Capability (VMUIF only)
- Receive Composed Messages
- Auto Logon
- Broadcast Capability
- Network Broadcast Capability (MMUI only)
- Administrator Capability (MMUI only)
- Auto Deletion of Invalid PDL Addresses (MMUI only)
- Personal Verification Changeable by User (MMUI only)
- Delivery to Non-User Capability (Outcalling feature)

- Send Message via DNU if Mailbox Not Found (Outcalling feature)
- Remote Notification Capability (Outcalling feature)
- Remote Notification Keypad Interface (MMUI only, Outcalling feature)
- Receive AMIS Open Network Messages (AMIS feature)
- Compose/Send AMIS Open Network Messages (AMIS)
- Message Waiting Indication Options

Finding, listing, and printing local voice users

Introduction

You can enter many different combinations of search criteria in the Find Local Voice Users screen.

The procedure that begins on page 9-68 is generic and applies to all types of searches. Several examples follow this procedure to show you how you would perform certain kinds of searches.

Purpose

You can use the find function in order to

- list the found users on the screen
- print a list of the found users
- reassign the found users to another class of service
- view or modify any of the found local voice users
- delete any of the found local voice users
- record a personal verification for any of the found local voice users

Reassigning users to another COS

If you want to reassign found local voice users to another class of service, see “Reassigning a subset of local voice users to another class of service” on page 9-71, and use that procedure instead of this one.

Specifying search criteria

You only need to change a search field if that field is part of your search criteria. All other fields should be left so that they display their default setting (blank or Any). When you leave a field at its default setting, it is disregarded in the search.

Example

You want to find all users in a particular department that have remote notification capability. You leave all other fields set to their default values.

Since, for example, Delivery to Non-User capability was not changed from its default value of Any, users that have it enabled and users who do not have it enabled will be found. Delivery to Non-User capability is not a relevant search criteria.

Procedure

This is a generic procedure that describes the steps to perform any kind of search.

Starting Point: The Find Local Voice Users screen

Step	Action
1	Determine the search criteria that will find all of the users you are looking for.
2	Fill in the necessary fields in order to define your search criteria. **Note:** Field descriptions begin on page 9-51.
3	Select the format in which you want to display or print the list of found users.

IF you want to	THEN set
see the following information • mailbox number • department • COS number • storage used • if the user has a personal verification	the Display the List in MWI Status Format field to No.
see the following information • DN • mailbox number • number of read messages • number of unread messages • number of text messages • the MWI status	the Display the List in MWI Status Format field to Yes.

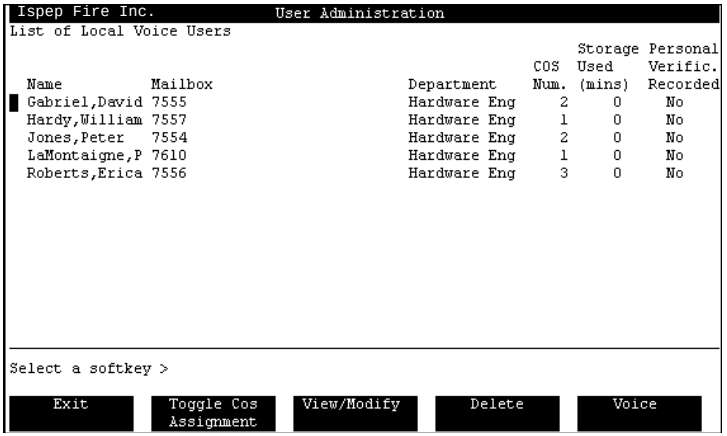
Step	Action
4	List, print, or assign found users to another class of service.

IF you want to	THEN
list the found users	go to step 5.
print the found users	go to step 8.
assign found users to another COS	go to page 9-71.
cancel the search	press [Exit].

Step	Action

5 Press the [List] softkey.

Result: The List of Local Voice Users screen is displayed.



6 Do you want to modify or delete a local voice user or record a personal verification?

- If yes, go to step 7.
- If no, press [Exit] to return to the Find Local Voice Users screen.

7 Select the user by moving your cursor to the user's name and pressing the <spacebar>.

IF you want to	THEN press	AND go to
view or modify a local voice user	[View/Modify]	page 9-78.
delete a local voice user	[Delete]	page 9-95.
record a personal verification for the user	[Voice]	page 9-32.

8 Press the [Print] softkey.

Result: The Printing softkeys are displayed.

9 Do you want to continue printing?

- If yes, press the [Continue Printing] softkey.

  Note: You can stop printing once started by pressing [Cancel Printing].
- If no, press the [Cancel Printing] softkey.

Example 1

You want to find and print all users in the Marketing department who have exceeded their voice storage limit.

Step	Action
1	Enter Marketing in the Department field.
2	Set Voice Storage Limit Exceeded to Yes.
3	Do you want the list in MWI status format? • If yes, set the Display the List in MWI Status Format field to Yes. • If no, set the Display the List in MWI Status Format field to No.
4	Press [Print]. **Result:** A list of the found users is printed.

Example 2

You want to find and list all users assigned to class of service 12 who have not recorded a personal verification.

Step	Action
1	Enter 12 in the COS field.
2	Set Personal Verification Status to Not_Recorded.
3	Do you want the list in MWI status format? • If yes, set the Display the List in MWI Status Format field to Yes. • If no, set the Display the List in MWI Status Format field to No.
4	Press [List]. **Result:** The found users are listed on the screen.

Reassigning a subset of local voice users to another class of service

When to use

Use this procedure when you want to

- find a group of local voice users that meet a certain set of search criteria and reassign them to another class of service
- find all users in a particular class of service and reassign them to a different class of service

Toggle COS assignment

If you want to reassign users who meet a certain set of search criteria to another class of service, you should verify the list of found users before you actually reassign them.

You may find that you have not found all required users, in which case you will have to redefine the search criteria; or, you may find that you have found some users who you do not want to reassign.

If you do not want to reassign some of the found users to another class of service, you can use the [Toggle COS Assignment] softkey to deselect them.

Reassigning users from one COS to another

If you want to reassign users from one class of service to another, you must enter the class of service number in the COS field. You will not be able to use any of the other class of service fields in the Find Local Voice Users screen. For a list of these fields, see “Restrictions on how you can combine search criteria” on page 9-65.

Reassigning users to another COS

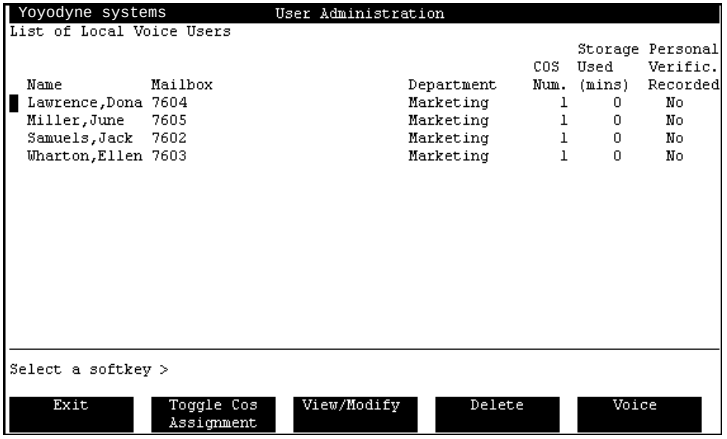
To reassign found local voice users to another class of service, follow these steps.

Starting Point: The Find Local Voice Users screen

Step	Action
1	Do you want to reassign users in one class of service to another class of service? • If yes, enter the users' current class of service number in the COS field and go to step 11. • If no, go to step 2.
2	Fill in the necessary fields to define your search criteria. **Attention:** If you enter a number in the COS field, you cannot use any of the other class of service fields in this screen. **Note:** Field descriptions begin on page 9-51.
3	Select the format in which you want to display or print the list of found users.

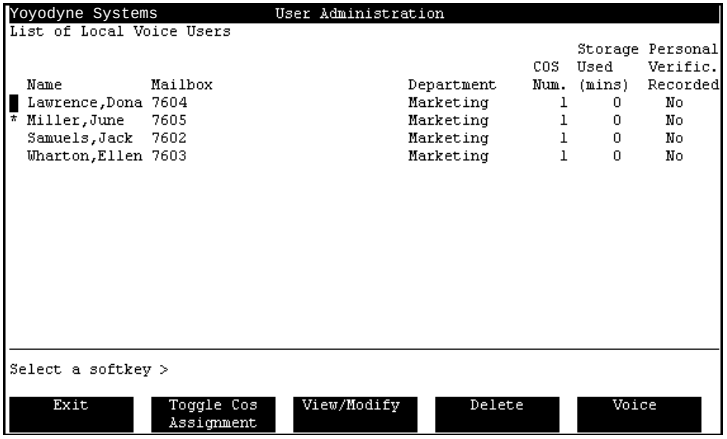
IF you want to	THEN set
see the following information • mailbox number • department • COS number • storage used • personal verification status	the Display the List in MWI Status Format field to No.
see the following information • DN • mailbox number • number of read messages • number of unread messages • number of text messages • the MWI status	the Display the List in MWI Status Format field to Yes.

Step	Action
4	Press the [List] softkey. **Result:** The List Local Voice Users screen is displayed.


Yoyodyne systems User Administration
List of Local Voice Users
Name Mailbox Department COS Num. Storage Used (mins) Personal Verific. Recorded
Lawrence,Dona 7604 Marketing 1 0 No
Miller,June 7605 Marketing 1 0 No
Samuels,Jack 7602 Marketing 1 0 No
Wharton,Ellen 7603 Marketing 1 0 No
Select a softkey >
Exit
Toggle Cos Assignment
View/Modify
Delete
Voice

5	Does the list contain all of the users you want to reassign? • If yes, go to step 6. • If no, redefine the search criteria. Press [Exit] to return to the Find screen, and repeat steps 2 to 4 until all users you want to reassign have been found.
6	Does the list contain any users *who you do not want* to reassign to another class of service? • If yes, go to step 7. • If no, go to step 10.
7	Select the user you do not want to reassign by moving your cursor to the user's name and pressing the spacebar. **Result:** The user is highlighted.

Step	Action
8	Press the [Toggle COS Assignment] softkey. **Result:** An asterisk appears next to the user's name. This asterisk indicates that the user will not be reassigned to the new class of service.


Yoyodyne Systems User Administration
List of Local Voice Users
Name Mailbox Department COS Num. Storage Used (mins) Personal Verific. Recorded
Lawrence,Dona 7604 Marketing 1 0 No
* Miller,June 7605 Marketing 1 0 No
Samuels,Jack 7602 Marketing 1 0 No
Wharton,Ellen 7603 Marketing 1 0 No
Select a softkey >
Exit
Toggle Cos Assignment
View/Modify
Delete
Voice

9	Are there any other users you do not want to reassign? • If yes, repeat steps 7 to 8 until you have deselected all users you do not want to reassign. • If no, go to step 10.
10	Press [Exit] to return to the Find Local Voice Users screen.
11	Press [Assign to COS] to reassign the found users. **Result:** You are prompted for a COS number.
12	Enter the number of the class of service to which you want to reassign the users and press Return. **Result:** As users are reassigned, a message is displayed, counting each user who is added to the new class of service.
13	If you want to abort the operation at any time, press the [Abort] softkey. **Result:** This stops the reassignment. However, it cannot undo any users who have already been reassigned.

When reassignment is complete

Once all users have been reassigned to the specified class of service, a message and a SEER are sent, stating that the COS assignment is complete. This message and SEER also report the number of users who were assigned and the number of users who failed to be reassigned.

Section C: Modifying and deleting local voice users

In this section

Accessing the View/Modify Local Voice User screen	9-78
Viewing and modifying a local voice user	9-82
Checking a user's status	9-84
Enabling a disabled mailbox	9-89
Changing a user's password	9-91
Monitoring mailbox logins for suspected hacker activity	9-92
Reassigning a mailbox to another user	9-94
Deleting a local voice user	9-95

Accessing the View/Modify Local Voice User screen

Introduction

You may or may not know the mailbox number of the user you want to view or modify. Use this table to decide which procedure to follow to access the View/Modify Local Voice User screen.

IF	THEN follow
you know the user's mailbox number	the procedure on this page.
you do not know the user's mailbox number	the procedure on page 9-79.

Before you begin

Since all users belong to customer groups, you must first access the customer group to which the user belongs. See "Selecting a customer to view or modify" on page 5-17.

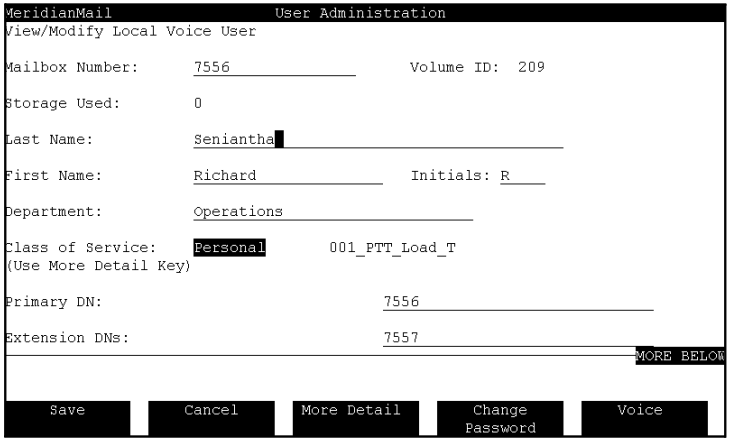
Accessing the screen when you know the mailbox number

To access the View/Modify Local Voice User screen directly, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.

Step	Action
4	Enter the user's mailbox number and press <Return>. **Result:** The View/Modify Local Voice User screen is displayed.



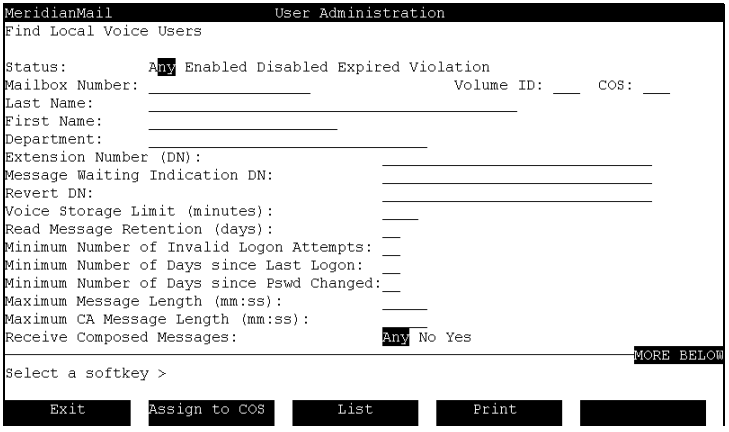
Finding a local voice user and accessing the screen

To find the local voice user you want to modify when you do not know the mailbox number, follow these steps.

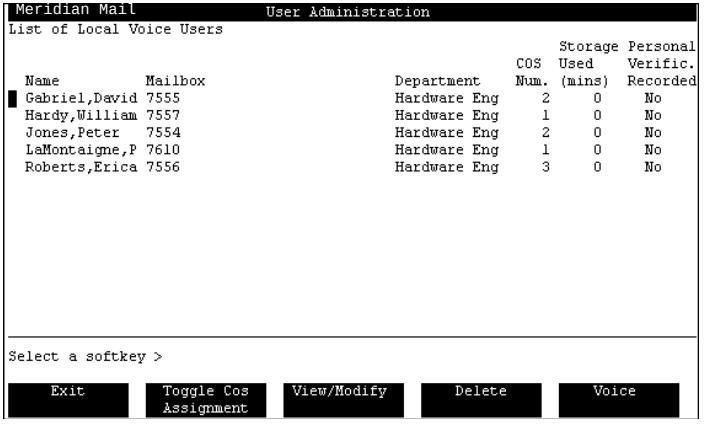
Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.

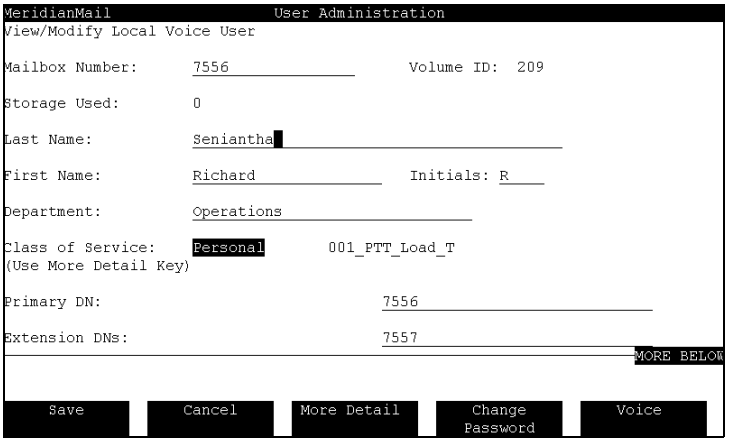
Step	Action
3	Press [Find]. **Result:** The Find Local Voice Users screen is displayed.



4	Enter the information you know about the user.
5	Press [List]. **Result:** The List of Local Voice Users screen is displayed.


Meridian Mail User Administration
List of Local Voice Users
Name Mailbox Department COS Num. Storage Used (mins) Personal Verific. Recorded
Gabriel,David 7555 Hardware Eng 2 0 No
Hardy,William 7557 Hardware Eng 1 0 No
Jones,Peter 7554 Hardware Eng 2 0 No
LaMontaigne,P 7610 Hardware Eng 1 0 No
Roberts,Erica 7556 Hardware Eng 3 0 No
Select a softkey >
Exit
Toggle Cos Assignment
View/Modify
Delete
Voice

Step	Action
6	Select the user you want to view or modify by moving your cursor to the user's name and pressing the spacebar.
7	Press [View/Modify]. **Result:** The View/Modify Local Voice User screen is displayed.



Viewing and modifying a local voice user

Introduction

Once you access the View/Modify Local Voice User screen, it functions exactly like the Add Local Voice User screen. Most of the procedures are, therefore, in Section A:: Adding local voice users. Several procedures that are unique to modifying an existing local voice user are described in this section. These are

- changing the user's last name
- enabling a disabled mailbox
- changing the user's password

Deciding what you need to modify

Use this table to decide what you need to modify in the user profile, and then find the page.

IF you want to	THEN go to
check the user's status	page 9-84.
change other user information (such as department)	page 9-14.
reassign the user to another class of service	page 9-17.
reassign a subset of users to another class of service	page 9-71.
create a personal class of service	page 9-19.
modify the revert DN, MWI DN, or extension DNs	page 9-29.
record a personal verification for a user	page 9-32.
create a remote notification schedule for a user	page 9-34.
monitor a mailbox for suspected hacker activity	page 9-92.
modify any of these local voice user characteristics: • name dialable by external callers • hospitality user class (if Hospitality is installed) • volume level (VMUIF only) • preferred language (multilingual systems only)	page 9-37.

IF you want to	THEN go to
enable a disabled mailbox	page 9-89.
change a user's password	page 9-91.
reassign a mailbox to another user	page 9-94

Procedure

To modify a local voice user, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Look up the type of change(s) you need to make in the table on page 9-82, and go to the page that is indicated for instructions.
2	Make the necessary changes.
3	Press the [Save] softkey.

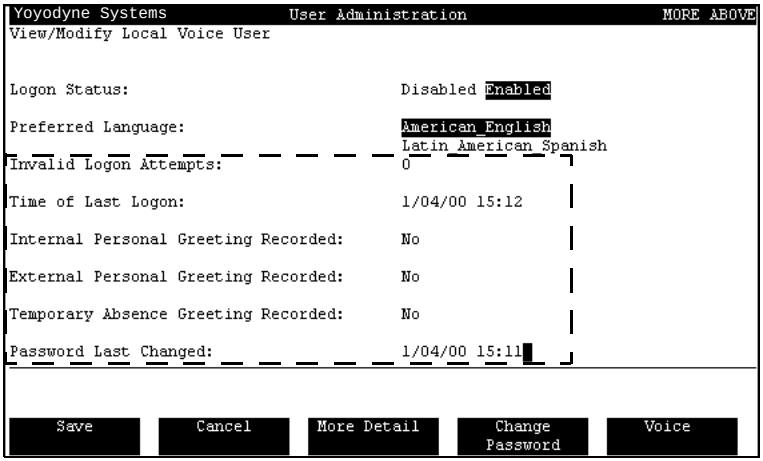
Checking a user's status

Introduction

The View/Modify Local Voice Users screen contains a number of status fields that are not displayed in the Add Local Voice Users screen. These are read-only information fields.

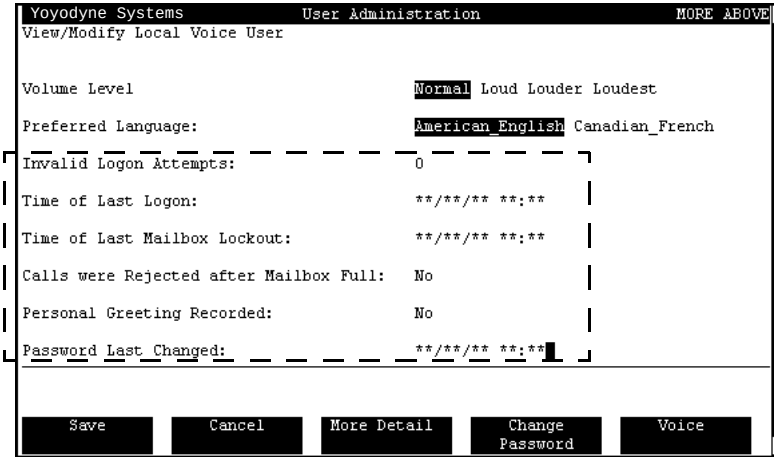
MMUI user status fields

The dotted box highlights the status fields that are displayed in the MMUI version of the screen.



VMUIF user status fields

The dotted box highlights the status fields that are displayed in the VMUIF version of the screen.



Field descriptions

The following are descriptions of the status fields that are displayed in the View/Modify Local Voice Users screen.

Invalid Logon Attempts	
Description	This is the number of successive logon attempts that have been made using an incorrect password. This field is reset to 0 when • a valid password is entered and the user is allowed to log in • you reenable the mailbox (if it has been disabled due to too many invalid logon attempts)
Potential security risk	A high number in this field can indicate that a hacker has been trying to get into this mailbox.
More information	See the section "Controlling access to Meridian Mail mailboxes" on page 7-123.

Time of Last Logon	
Description	This is the time at which the user last logged in to his or her mailbox. A series of asterisks indicates that the user has not logged in.
Potential security risk	If a considerable amount of time has passed since the user's last logon, you may want to investigate why this is the case. It could be that • the user is on holiday or extended leave • the user has forgotten his or her password and has not notified you • the user has left the organization (in which case the mailbox should be deleted for security reasons)

Time of Last Mailbox Lockout	
Description	If the user has been locked out of his or her mailbox, this is the time at which the last lockout occurred.
Interface	VMUIF only
Potential security risk	VMUIF users are locked out of their mailboxes after an excessive number of invalid logon attempts. Lockout could indicate that a hacker has been trying to get into this mailbox.
More information	See the section "Controlling access to Meridian Mail mailboxes" on page 7-123.

Calls Rejected after Mailbox Full

Description	*Yes* indicates that the user's mailbox became full and that call answering messages were rejected as a consequence. *No* indicates that calls have not been rejected.
Interface	VMUIF only
Voice storage limit	If a user complains of many lost messages, consider reassigning him or her to another class of service that has a higher voice storage limit. This will allow more messages to be deposited in the mailbox before becoming full.

Personal Greeting Recorded

Description	This field indicates whether the user has recorded a personal greeting.
Interface	VMUIF only

Internal Greeting Recorded

Description	This field indicates whether the user has recorded an internal greeting. This greeting is played to internal callers when they are transferred to Meridian Mail to leave a message.
Interface	MMUI only
Interaction with external greeting	This table indicates which greeting is played to internal callers.

WHEN	THEN
there is an internal greeting	the internal greeting is played.
there is no internal greeting but there is an external greeting	the external greeting is played.
there is no internal greeting and no external greeting	a standard system greeting is played.

External Personal Greeting Recorded	
Description	This field indicates whether the user has recorded an external greeting. The external greeting is played to external callers (or internal callers if no internal greeting is recorded) when they are transferred to Meridian Mail.
Interface	MMUI only

Temporary Absence Greeting Recorded	
Description	This field indicates whether the user has recorded a temporary absence greeting. If this greeting is recorded, it is played to internal and external callers until the expiry date.
Interface	MMUI only

Temporary Absence Greeting Expiry Date	
Description	If a temporary absence greeting has been recorded, this field is displayed to indicate when that greeting will expire.
Interface	MMUI only
Possible Values	A date and time indicate that the user has defined an expiry date for the greeting. *Indefinite* indicates that the user has not defined an expiry date for the greeting.
Expired greetings	If the current date has passed the expiry date, the field will be followed by the word "Expired."

Password Last Changed	
Description	This field indicates when the user last changed his or her password. Both the date and time are displayed.
MMUI versus VMUIF	When a new VMUIF user is added, this field is set to Nil. For users who were added a while ago, Nil indicates that they have not changed their default passwords. When a new MMUI user is added, this field is set to the time at which the user was added.

Enabling a disabled mailbox

Introduction

If too many invalid logon attempts are made to a mailbox and the Maximum Invalid Logon Attempts Permitted per Mailbox (as defined in the Voice Security Options screen) is reached, that user's mailbox is disabled.

What happens: MMUI users

When there are too many invalid logon attempts to the mailbox, the mailbox is disabled.

The MMUI user cannot log on to his or her mailbox, but messages are still recorded. When the user's mailbox is reenabled, he or she will be able to listen to the messages that were received while the mailbox was disabled.

What happens: VMUIF users

When there are too many invalid logon attempts on a VMUIF user's mailbox, the following happens:

- The mailbox is disabled.
- The Time of Last Mailbox Lockout field in the View/ Modify Local Voice User screen displays the time at which the mailbox was disabled.
- Meridian Mail checks the Lockout Duration field in the user's class of service to see how long the user should be locked out.

While a VMUIF user's mailbox is disabled, the user can logon, but calls are rejected and new messages are not recorded.

Deciding if action is needed for VMUIF users

For VMUIF users who have been locked out of their mailbox, you may or may not have to manually reenable the mailbox.

IF the Lockout Duration is	THEN
00.00	you must manually reenable the user's mailbox.
not 00.00	you do not have to manually reenable the mailbox. The mailbox is automatically reenabled after the lockout period has passed.

Potential security risk

A high number of invalid logon attempts could be an indicator that a hacker has been attempting to get into your system through this user's mailbox.

Contact the user and investigate why so many invalid logon attempts were made. If the user does not think he or she was responsible for these attempts, you should monitor this user's mailbox for future logon attempts.

Procedure

To enable a disabled mailbox, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Go to the Logon Status field and set it to Enabled.
2	Do you suspect hacker activity? • If yes, set the Monitor Mailbox during Monitoring Period field to Yes. • If no, go to step 3. **Note:** See "Monitoring mailbox logins for suspected hacker activity" on page 9-92.
3	Press [Save]. **Result:** The mailbox is reenabled and the Invalid Logon Attempts field is reset to 0.
4	Notify the user that his or her mailbox has been reenabled.

Changing a user's password

When to use

If a local voice user has forgotten his or her password, you will have to change it at the administration terminal.

Procedure

To change a user's password, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Press the [Change User Password] softkey. **Result:** You are prompted for a new password.
2	Enter the new password and press <Return>. **Note:** This password must contain numbers only. It can be up to 16 digits in length. **Result:** You are prompted to reenter the password for verification.
3	Enter the same password and press <Return>.
4	Did you get a message indicating a mismatch between the two passwords you entered? • If yes, repeat steps 2 to 3 until there is no mismatch. • If no, go to step 5.
5	Press [Save].
6	Inform the user of the new password.

Monitoring mailbox logins for suspected hacker activity

Introduction

Hacker Monitor is a new feature that flags hacker activity by issuing information SEERs to bring your attention to suspicious activity. Since mailboxes are a potential security risk, mailbox logins are one type of activity that you should check using Hacker Monitor.

When to use

Typically, you do not need to turn mailbox monitoring on for new users. Turn it on only if you suspect that a hacker has been using a particular mailbox. You may, for example, get complaints of abusive messages being sent from a particular mailbox. This is an indication of potential hacker abuse.

How it works

A monitoring period is defined in the Voice Security Options screen. This is the time period during which logins will be monitored.

If mailbox monitoring is enabled, every time someone logs in to the mailbox during the monitoring period, a SEER will be issued. For MMUI users, SEER 2262 will be issued, whereas for VMUIF users, SEER 5662 will be issued.

Procedure

To enable mailbox monitoring, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Obtain the times when the suspected hacker uses the system. **Note:** You can do this from Meridian 1 CDR records, or from Meridian Mail Reporter.
2	Is the monitoring period set up to reflect these times? • If yes, go to step 5. • If no, go to step 3.
3	Select Voice Administration and then Voice Security Options.
4	Enter the time period in the System Access Monitoring Period field, save your change, and return to the Customer Administration Menu.

Step	Action
5	Select User Administration.
6	Select Local Voice User and press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.
7	Enter the user's mailbox number.
8	Go to the Monitor Mailbox during Monitoring Period field and set it to Yes.
9	Press the [Save] softkey. **Result:** Whenever the mailbox is logged into during the monitoring period, SEER 2262 for MMUI users or SEER 5662 for VMUIF users will be generated.

Immediate notification of login

If you (or a support person) want to be notified immediately of an occurrence of these SEERs, you can set up a SEER message trigger mailbox and then enable remote notification for that mailbox. To do this you must do the following.

1. Enable mailbox monitoring as described above.
2. Set up a message trigger for SEER 2262 or 5662, or both, so that an urgent SEER message is deposited in a designated mailbox when the mailbox is logged into.

   See "Using SEER triggering" on page 30-35.
3. Set up remote notification for the designated mailbox so that you (or a support person) will be paged or phoned as soon as the urgent message is deposited.

   Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for more information.

Reassigning a mailbox to another user

Two methods

There are two methods for reassigning a mailbox from one user to another. They are:

- modify the mailbox, changing the appropriate fields (Name, Title, Department, etc.) from the old user's data to the new user's data
- delete the mailbox, then re-add it, filling in the new user's data as you configure the mailbox

First method: modify the mailbox

If you use this method, Operational Measurements will not differentiate between traffic/usage associated with the old user and traffic/usage associated with the new user. The reports will supply statistics for that mailbox as if no change had been made.

To use this method, see "Viewing and modifying a local voice user" on page 9-82 for details on how to modify the mailbox.

Second method: delete and add the mailbox

If you use this method, Operational Measurements reports will present the statistics for the old user separately from the statistics for the new user, even though the mailbox number is the same for both.

To use this method, follow the steps below.

1. Contact the current owner of the mailbox and make sure he or she has listened to all of his or her messages.
2. Access the Delete Local Voice User screen and delete the local voice user.

   See "Deleting a local voice user" on page 9-95.
3. Add a new local voice user, using the same mailbox number, and enter the new user's information.

   See "Accessing the Add Local Voice User screen" on page 9-9.

Deleting a local voice user

When to use

You will have to delete a local voice user when

- reassigning the mailbox to another user
- a user leaves the company

Potential security risk

When a user leaves the company, be sure to delete the mailbox immediately. An unused mailbox is a security risk since it is forgotten about and suspicious activity often goes unnoticed.

Choosing the correct procedure

You may or may not know the mailbox number of the user you want to delete. Use this table to decide which procedure to follow to access the Delete Local Voice User screen and then delete a user.

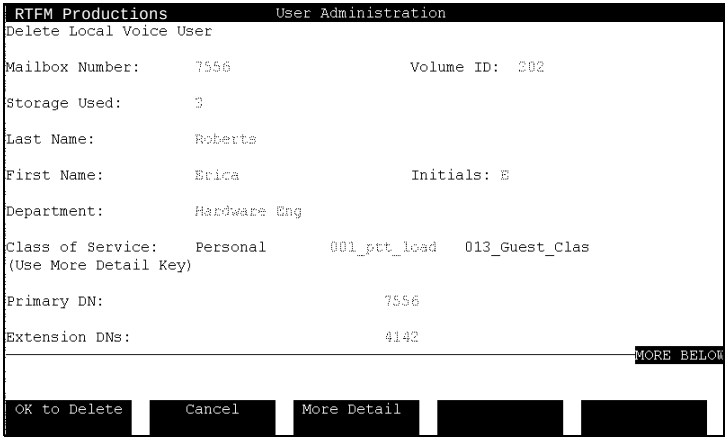
IF	THEN follow
you know the user's mailbox number	the procedure on page 9-96.
you do not know the user's mailbox number	the procedure on page 9-97.

Deleting a local voice user when you know the mailbox number

To delete a local voice user when you know the user's mailbox number, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [Delete] softkey. **Result:** You are prompted for the mailbox number.
4	Enter the mailbox number and press <Return>. **Result:** The Delete Local Voice User screen is displayed.



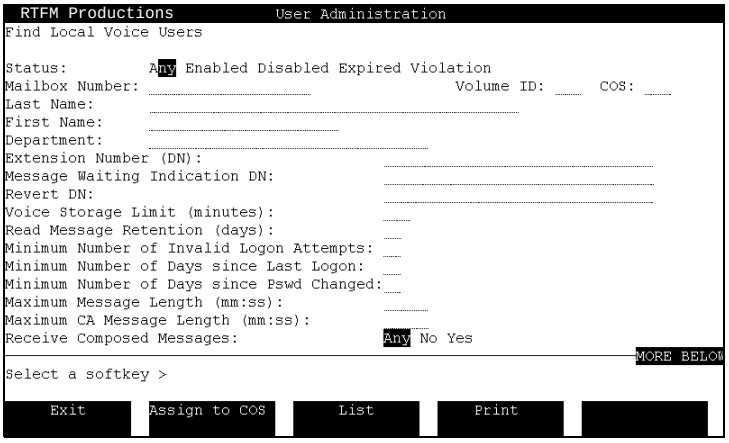
Step	Action
5	Is this the user you want to delete? • If yes, go to step 6. • If no, press [Cancel] and abandon the procedure. Obtain the correct mailbox number or use the next procedure on page 9-97 to find the user.
6	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.
7	Do you want to delete another local voice user? • If yes, repeat steps 4 to 6 until you have deleted all local voice users that you need to delete at this time. • If no, press the [Cancel] softkey.

Finding and deleting a local voice user

To find a local voice user you want to delete when you do not know the mailbox number, follow these steps.

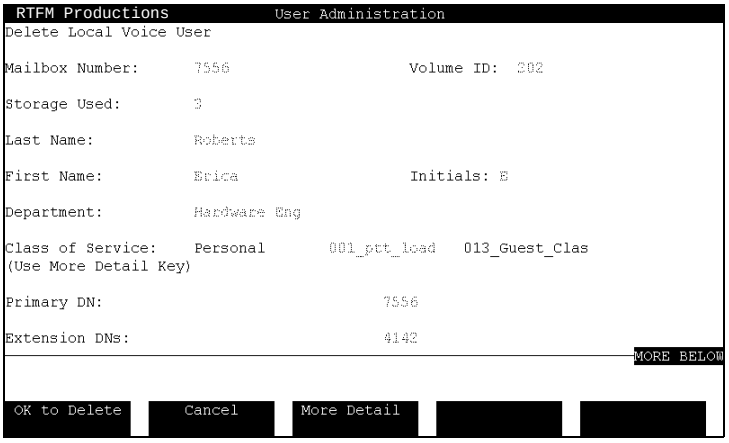
Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press [Find]. **Result:** The Find Local Voice Users screen is displayed.



4	Enter the information you know about the user. **Examples:** Last Name, First Name, Department
5	Press [List].

Step	Action
6	Select the user you want to view or modify by moving your cursor to the user's name and pressing the spacebar.
7	Press [Delete]. **Result:** The Delete Local Voice User screen is displayed.



8	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.

Chapter 10

Remote voice users

In this chapter

Section A: Introduction	10-3
Section B: Adding remote voice users	10-11
Section C: Finding remote voice users	10-27
Section D: Modifying and deleting remote voice users	10-39

Section A: Introduction

In this section

What is a remote voice user?	10-4
Remote voice user changes and enhancements	10-6
Permanent remote voice users	10-8
Temporary remote voice users	10-9

What is a remote voice user?

Definition

A remote voice user (RVU) is a Meridian Mail user whose mailbox resides on a remote networking site and who has been added to the local site's user database.

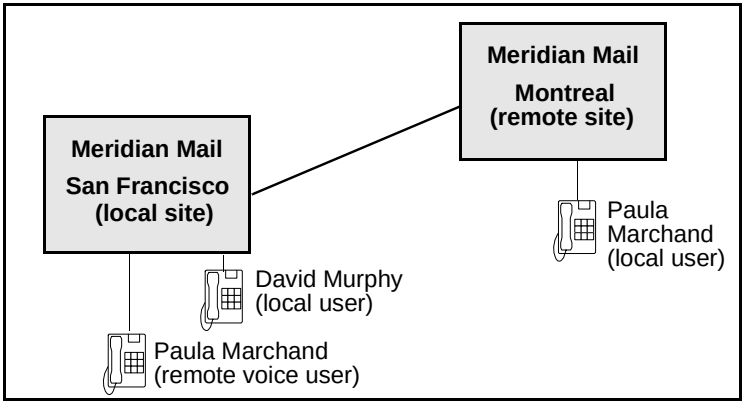
Benefits

The benefits of adding users from remote sites as remote voice users in the local site are as follows.

- Whenever a user at the local site addresses a message to a remote voice user, the remote voice user's personal verification (spoken name) is played.
- Local users can use the name dialing and name addressing features to call and compose messages to remote voice users.
- While listening to a voice message left by a remote voice user, a local user can use call sender (press 9 on the keypad) to immediately call back the originator of the message.
- External callers can name-dial remote voice users (if this feature is enabled).
- Remote voice users can be added to system and personal distribution lists.

Example

David Murphy is a local user at your San Francisco Meridian Mail site. Paula Marchand is a user at the remote Montreal Meridian Mail site. Paula has been added to your local site as a remote voice user.



Example (cont'd)

David Murphy can use name addressing when composing a voice message to Paula Marchand. During message addressing, David will hear Paula's spoken name as a verification of the mailbox number he has entered.

When David listens to a voice message received from Paula, he presses 9 (call sender) to call Paula back.

Remote voice user changes and enhancements

Introduction

In recent Meridian Mail releases, a number of enhancements have been made to the administration of remote voice users to

- provide support for remote voice user propagation to other sites
- to simplify the management of the remote voice user database

New type of remote voice user

In Meridian Mail Releases 11 and 12, you can add remote voice users as temporary users. In the past, users at remote sites could only be added as permanent remote voice users. They had to be added and deleted manually, one at a time.

Temporary users can be added and deleted automatically by the system.

Simplified addition of remote voice users

Prior to Meridian Mail 11, you had to enter each remote voice user to your local site one user at a time.

Now, you can quickly and easily add remote voice users in one of two ways.

- RVU Propagation via Enterprise Networking automatically adds remote voice users to your local site whenever a user at a remote site addresses a voice message to a user at your local site. These users are added as temporary users.
- RVU Propagation via Bulk Provisioning allows you to copy all (or a subset of) users at a remote site to tape and then copy them into your local database as remote voice users. These users can be added as temporary or permanent.

Personal verification in user's voice

Prior to Meridian Mail 11, personal verifications (spoken names) for remote voice users could only be recorded by the local administrator, and, therefore, in a voice other than the user's.

In Meridian Mail Releases 11 and 12, when temporary remote voice users are added to the system using RVU Propagation, the personal verification of each user is added in that user's voice, provided that the user has recorded a personal verification.

When the personal verification is played for remote voice users

A personal verification is played for remote voice users in the following situations:

- A local user composes a message to a remote voice user. When the user enters the remote user's mailbox (or name if using name addressing), he or she will hear the remote voice user's personal verification in the user's voice.
- A local user name dials a remote voice user.
- A local user uses the call sender feature on a message from a remote voice user.
- The envelope of a message received from a remote voice user is played.

When no personal verification has been recorded for a remote voice user

When no personal verification has been recorded, the system plays the remote site's spoken name and the mailbox number (for example, *"Maidenhead, mailbox 1334."*)

If there is no spoken name recorded for the remote site, the system plays the mailbox number in network format (for example, *"Mailbox 64441334."*)

Permanent remote voice users

Introduction

All remote voice users that existed prior to Meridian Mail Release 11 were permanent remote voice users. As of Meridian Mail 11, remote voice users can still be added as permanent remote voice users.

Adding permanent users

Permanent remote voice users can be added in one of two ways.

User Administration

They can be added one at a time through User Administration. This is the way you had to enter them prior to Release 11.

See “Adding remote voice users through User Administration” on page 10-17.

Bulk Provisioning

You can use the Bulk Provisioning feature to copy users from a remote site to your local site’s database as permanent remote voice users.

See “Adding remote voice users using RVU Propagation via Bulk Provisioning” on page 10-24.

Deleting permanent users

Permanent remote voice users remain on the system until you delete them. Permanent users must be deleted one at a time through the User Administration menu.

See “Manually deleting remote voice users” on page 10-45.

Making permanent users temporary

You can convert permanent remote voice users who have not been active for a long time to temporary remote voice users and allow the system to take care of deleting inactive users.

You can verify when a user was last active in one of two ways.

- Check the Last Access Time field in the View/Modify Remote Voice User screen.
- Use the Find function and list all permanent remote voice users. You can then select and modify users from the List screen.

Temporary remote voice users

Introduction

Temporary remote voice users were also introduced in Meridian Mail 11. Temporary remote voice users make administration of remote voice users much easier since they can be both added and deleted automatically by the system.

Adding temporary users

Temporary remote voice users can be added in one of three ways.

User Administration

You can add temporary remote voice users one at a time through User Administration in the same way that you add permanent users.

See “Adding remote voice users through User Administration” on page 10-17.

RVU Propagation via Enterprise Networking

You can have remote voice users automatically added to your system when they send network messages to the local site.

When temporary users are added this way, the personal verifications that users have recorded in their own voices are used.

See “Adding temporary remote voice users using RVU Propagation via Enterprise Networking” on page 10-21.

RVU Propagation via Bulk Provisioning

You can also use the Bulk Provisioning feature to copy users from a remote site to tape and then to your local site’s database as temporary or permanent remote voice users. This method is not automatic, but it does allow you to quickly add all users (or a subset of users) from a remote site to your local database.

When remote voice users are added this way, the personal verifications that users have recorded in their voice are used.

See “Adding remote voice users using RVU Propagation via Bulk Provisioning” on page 10-24.

Deleting temporary users

Temporary remote voice users can be deleted in one of two ways.

Manual deletion

If you want to delete a particular remote voice user, you can do so through the User Administration menu in the same way that you delete permanent remote voice users.

See “Manually deleting remote voice users” on page 10-45.

Automatic deletion during nightly audits

Nightly audits are performed on the database of temporary remote voice users in order to keep it from getting too large.

Whenever the number of temporary remote voice users exceeds a threshold, the nightly audit removes the oldest temporary remote voice users in the system. If the number of temporary remote voice users reaches the maximum number allowed on the system, no more temporary users will be added by Remote Voice User Propagation until after the nightly audit is run.

See “How temporary remote voice users are automatically deleted from the system” on page 10-49.

Making temporary users permanent

If you do not want a particular temporary user to be deleted during a nightly audit, you can change that user to a permanent user. Permanent users are not deleted during the nightly audit.

See “Viewing and modifying remote voice users” on page 10-40.

Section B: Adding remote voice users

In this section

The Add Remote Voice User screen	10-12
Adding remote voice users through User Administration	10-17
Recording a personal verification for a remote voice user	10-19
Adding temporary remote voice users using RVU Propagation via Enterprise Networking	10-21
Adding remote voice users using RVU Propagation via Bulk Provisioning	10-24

The Add Remote Voice User screen

Introduction

Permanent and temporary remote voice users can be added to the system one at a time from this screen.

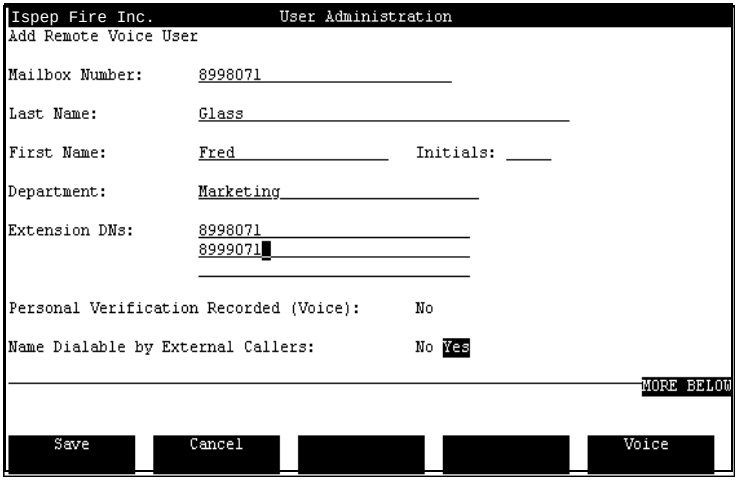
Administration level

Remote voice users can only be added from the Customer Administration level.

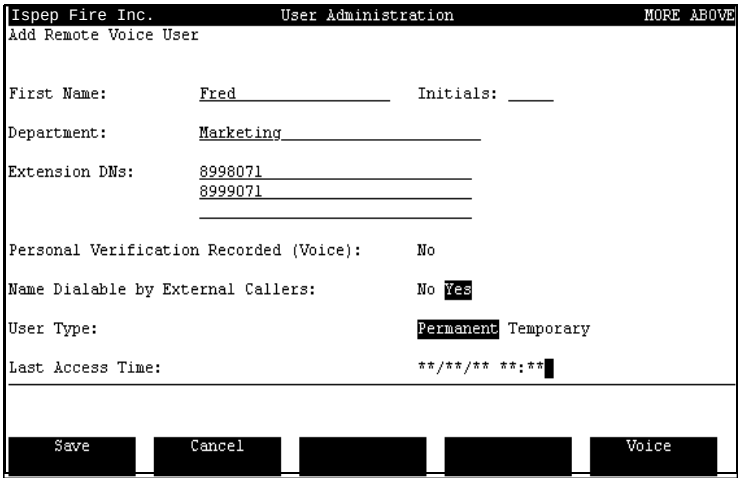
The screen

This is the Add Remote Voice User screen.

Part 1



Part 2



Field descriptions

This table describes the fields in the Add Remote Voice User screen.

Mailbox Number	
Description	The remote voice user's mailbox number.
Format	The mailbox number must be in network format. It must include the network prefix or steering code of the remote site.
Example	If the dialing plan is ESN, a valid mailbox number is 6233 4433, where 6233 is the network prefix and 4433 is the mailbox number. If the dialing plan is CDP, a valid mailbox number is 54433, where 54 is the steering code.
Default	The number you entered to access the Add Remote Voice User screen.
Maximum length	28 digits (including network prefix)
Mandatory	This field is mandatory. The user cannot be saved if this field is blank.

Last Name and First Name	
Description	The remote voice user's last and first names.
Maximum length	You can enter up to 41 characters for the last name and 21 characters for the first name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).
Attention	Make sure the spelling is correct. These fields are used by the name dialing and name addressing features. For this reason, it is recommended that you use only alphanumeric characters.

Initials	
Description	Initials can be used to distinguish users with identical first and last names. They are not used by the name dialing or name addressing features.
Default	If you leave this field blank, Meridian Mail will automatically insert the first letter of the user's first name when you save the user.
Maximum length	5 characters

Department	
Description	The remote voice user's department.
Default	This field is blank for the first user you add. For subsequent users, this field defaults to the department entered for the last user you added (as the [Cancel] softkey was not pressed).
Maximum length	31 characters
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).

Extension DNs	
Description	A user can have up to three extensions. This means that a caller can dial any one of these numbers and reach the user. The first field is for the primary DN.
Format	These DNs must be in network format. They must include the network prefix or steering code of the remote site.
Maximum length	30 digits
Default	The first DN field is typically filled in with the mailbox number you entered to access the Add Remote Voice User screen.
See Also	See “Primary DN and extension DNs” on page 9-21.

Personal Verification Recorded (Voice)	
Description	This read-only field indicates whether a spoken name has been recorded for this user (either by the user or by the administrator).
Default	This field is set to No when you first add a user.

Name Dialable by External Callers	
Description	This field determines whether this user can be name dialed by external callers. An external caller is anyone who is calling in from a phone that is not on your PBX.
Default	This field uses the setting for the Name Dialable by External Callers field in the Networking Configuration screen under the Network Administration menu.
Valid Options	Yes, No

User Type	
Description	This field identifies the type of remote voice user.
Default	Permanent
Valid Options	Permanent, Temporary
See Also	See “Permanent remote voice users” on page 10-8 and “Temporary remote voice users” on page 10-9.

Last Access Time	
Description	This is a read-only field that indicates the last time • the user was modified via User Administration • the user’s personal verification was played • an Enterprise Networking message was received from this user • the user was updated using bulk provisioning
Default	This field is set to the date and time at which the user is added.
Usage	This time-stamp is used by the nightly audit to determine which temporary remote voice users should be deleted when there are too many temporary users on the system.

Adding remote voice users through User Administration

When to use

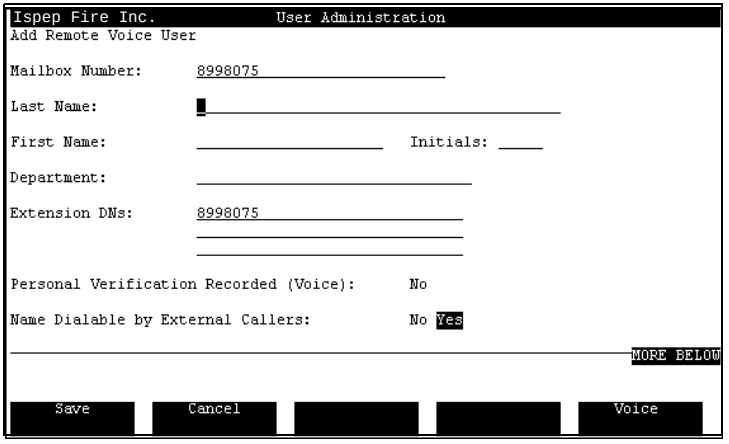
Use this procedure to add either permanent or temporary remote voice users one at a time.

Procedure

To add a remote voice user, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration. **Result:** The User Administration menu is displayed.
2	Select Remote Voice User.
3	Press the [Add] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the mailbox number of the remote voice user. **Requirement:** Enter the necessary network prefix or steering code as part of the mailbox number. **Result:** The Add Remote Voice User screen is displayed.



Note: Field descriptions begin on page 10-13.

5	Enter the user's last name and first name.
6	Enter the user's initials.
7	Enter the user's department.

Step	Action
8	Does the user have a phone and can he or she be dialed directly from the local site? • If yes, go to step 9. • If no, make all Extension DN fields blank and go to step 11.
9	Does the user have more than one extension DN? • If yes, go to step 10. • If no, go to step 11.
10	Enter the user's other DN(s) in the remaining Extension DN fields.
11	Do you want to record a personal verification (spoken name) for the user? • If yes, see "Recording a personal verification for a remote voice user" on page 10-19. • If no, go to step 12.
12	Do you want external callers to be able to name dial this user? • If yes, set the Name Dialable by External Callers field to Yes. • If no, set the Name Dialable by External Callers field to No.
13	Is this a permanent user? • If yes, select Permanent. • If no, select Temporary.
14	Do you want to save the user with the information you have entered? • If yes, press the [Save] softkey. • If no, press the [Cancel] softkey or make the necessary changes and then press [Save].

Recording a personal verification for a remote voice user

Introduction

Ideally, users should record personal verifications (spoken names) in their own voice. However, as administrator, you can record personal verifications from the administration terminal on behalf of users.

Administration level

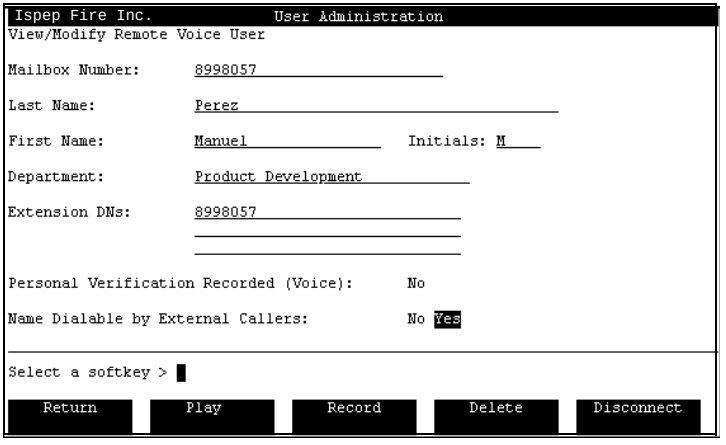
Recording a personal verification for a remote voice user can be done only from the Customer Administration level.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Remote Voice User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey. **Result:** You are prompted to enter the extension of the phone you want to use to record the verification.
3	Enter the extension of the phone and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.



Step	Action
5	Press the [Record] softkey. **Result:** The [Stop] softkey is displayed.
6	At the sound of the beep, speak the user's name (and, optionally, the user's extension). **Example:** *"Heather McGee at extension 8523."*
7	Press the [Stop] key to stop recording.
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.
9	Do you want to rerecord the verification? • If yes, repeat steps 5 to 8 to rerecord the verification. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.

Adding temporary remote voice users using RVU Propagation via Enterprise Networking

Introduction

The RVU Propagation via Enterprise Networking feature can be used to add temporary remote voice users.

When this feature is enabled, temporary remote voice users are added automatically.

Requirement

Enterprise Networking must be enabled on both sites: your local site *and* the remote site from which you want to add users to your system.

Enabling RVU Propagation via Enterprise Networking

To automatically add temporary remote voice users to your system, you must enable the RVU Propagation via Enterprise Networking feature. It is disabled by default.

This feature is enabled through Network Administration.

1. Enable RVU Propagation via Enterprise Networking for the local site.

   In the Networking Configuration screen of the local Meridian Mail site, set the Add/Update Remote Voice Users field to Yes.

   This informs Meridian Mail that you want to receive remote voice user information at the local site.

2. Choose the sites whose users you want added as remote voice users to your system. The sites you choose must be Enterprise Networking sites.

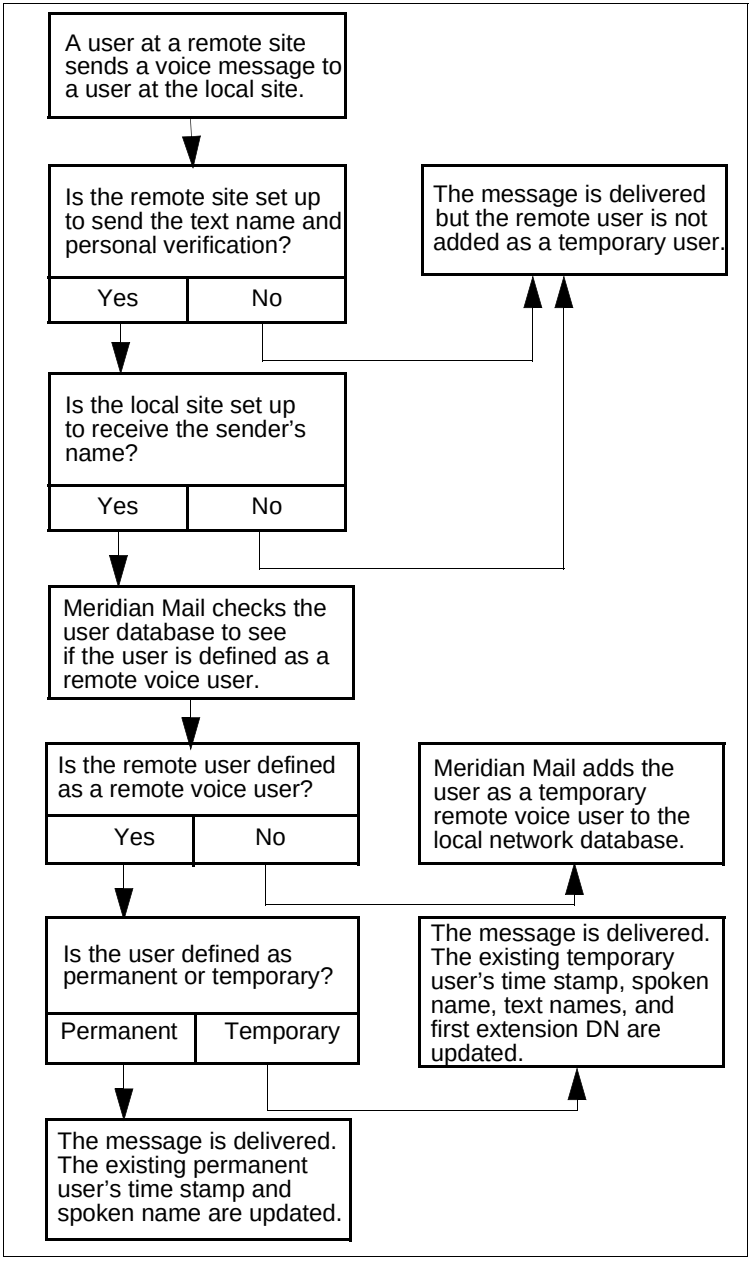
3. To enable the sending of RVU information from each remote site, you must set the Send the Sender's text name and personal verification field to Yes in the Remote Site Maintenance screen at the *remote* Meridian Mail system (not the local system).

See also

For detailed instructions on enabling this feature, refer to the *Enterprise Networking Guide* NTP (555-7001-246), "Maintaining the network" chapter.

When users are added/updated

A temporary remote voice user is added to the local site when a user at a remote site sends a network message to a user at the local site. Remote voice user information is taken from the header of the Enterprise network message that is received.


A user at a remote site sends a voice message to a user at the local site.
Is the remote site set up to send the text name and personal verification?
Yes
No
The message is delivered but the remote user is not added as a temporary user.
Is the local site set up to receive the sender's name?
Yes
No
Meridian Mail checks the user database to see if the user is defined as a remote voice user.
Is the remote user defined as a remote voice user?
Yes
No
Meridian Mail adds the user as a temporary remote voice user to the local network database.
Is the user defined as permanent or temporary?
Permanent
Temporary
The message is delivered. The existing temporary user's time stamp, spoken name, text names, and first extension DN are updated.
The message is delivered. The existing permanent user's time stamp and spoken name are updated.

Limitations

The following are limitations of the RVU Propagation via Enterprise Networking feature:

- Users at remote sites are added to your system as temporary remote voice users only when messages are received from them.

  Remote voice users who do not send network messages will not be added as remote voice users even if they are regularly name-dialed or have a lot of messages sent to them.

  For a description of how to work around this limitation, see "Application 2: Seeding temporary users" on page 10-25.
- No operational measurements are collected for remote voice users.
- If the sender's site does not have mailbox numbers that match the dialing plan, the call sender and name dialing features are not available.
- Additions and updates of temporary remote voice users is blocked during the nightly audit.
- Only 18 characters of the remote voice users text name will be sent.

WHEN	THEN
the first and last names are 18 characters or less	the first and last names of the user are sent.
the last name and initials are 18 characters or less	the last name and initials of the user are sent.
the last name only is 18 characters or less	only the last name is sent.
the last name is more than 18 characters long	only the last name is sent and is truncated to 18 characters.

Adding remote voice users using RVU Propagation via Bulk Provisioning

Introduction

Bulk Provisioning is a Meridian Mail 12 feature that allows you to transfer data between Meridian Mail systems using tapes. One of the ways in which you can use this feature is to copy local users from a remote site to tape and then to your local user database as temporary or permanent remote voice users.

Information that is added/updated

The following user information is added to the local system:

- the user's entire name
- the user's mailbox
- the user's primary DN
- the user's personal verification (spoken name)
- the user's department

Application 1: Provisioning permanent users

You can use this feature to add a large number of permanent remote voice users to your local user database. This eliminates the need to add each user manually.

The other benefit over adding each user manually, is that the personal verifications (spoken names) that users have recorded in their own voice will be used. This means that you no longer have to record users' personal verifications at the administration terminal.

Application 2: Seeding temporary users

RVU Propagation via Bulk provisioning

You can use bulk provisioning to initially add temporary remote voice users in a batch as the network is set up. In this way, all the users at a remote site could be made available at one time.

RVU Propagation via Enterprise Networking

Once users have been added using bulk provisioning, you can use RVU Propagation via Enterprise Networking to maintain the database of temporary users.

This means that any additional temporary remote voice users will automatically be added on an as-needed basis. Over time, the less frequently used temporary remote voice users will be deleted during the nightly audit to lessen the system load. Only regularly accessed temporary users will be kept on the system.

Application 3: Selective seeding of temporary users

In Application 2, you use RVU Propagation via Bulk Provisioning to seed a large number of temporary remote voice users.

If you want to add a selective (smaller) subset of remote voice users to your system, you can do the following.

1. Compose a voice message to the users you want to add as remote voice users to your system.
2. Tag the message for acknowledgment.
3. Send the message.

   When the read message acknowledgment comes back, the users are added as temporary remote voice users.

See also

For information about how to use the bulk provisioning feature, see Chapter 35, “Bulk provisioning”.

Section C: Finding remote voice users

In this section

Accessing the Find Remote Voice Users screen	10-28
The Find Remote Voice Users screen	10-29
Wildcard characters	10-32
Finding, listing, and printing remote voice users	10-34

Accessing the Find Remote Voice Users screen

Introduction

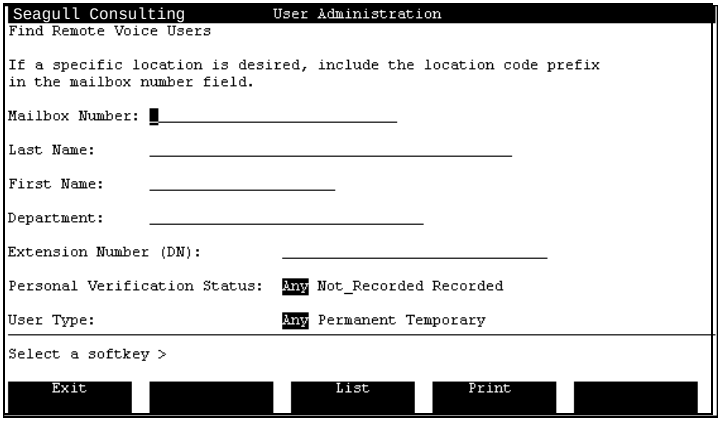
You fill in your search criteria in the Find Remote Voice Users screen. You can then choose to print or list (on screen) the users that are found. If you choose to view the list on screen, you can then select a user in order to view, modify, or delete the user.

Procedure

To access the Find Local Voice Users screen, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Find] softkey. **Result:** The Find Remote Voice Users screen is displayed.



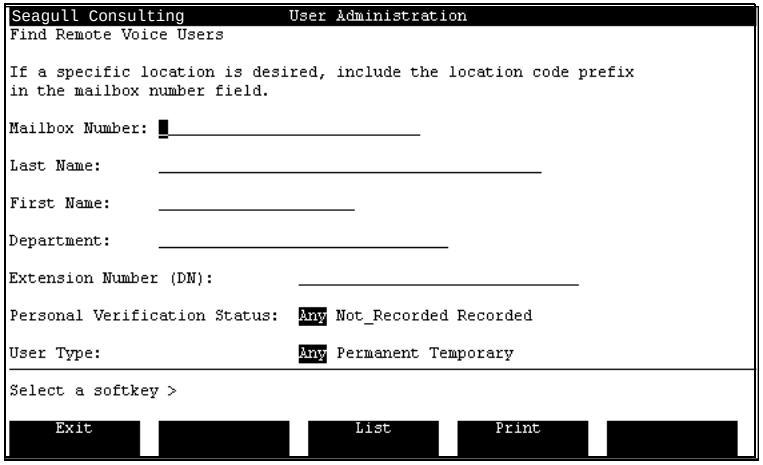
The Find Remote Voice Users screen

Introduction

By entering what you know about the user or subset of users you want to find, Meridian Mail will search the database and return a list of remote voice users that meet the criteria you have specified.

The screen

This is the Find Remote Voice Users screen.



Field descriptions

This table describes the fields in the Find Remote Voice Users screen.

Mailbox Number	
Description	Use this field to find users within a certain range of consecutive mailbox numbers or a particular user. To find a range of mailbox numbers, use the appropriate wildcards. The mailbox number must include the network prefix of the remote site.
Maximum Length	You can enter up to 28 characters.

Last Name	
Description	Use this field (in combination with the first name field) if you want to find a particular user, or alone to find all users with a particular last name. Use wildcards if you are unsure of the exact spelling.
Default	Blank (finds users with any last name)

First Name	
Description	Use this field (in combination with the last name field) to find a particular user, or alone to find all remote voice users with a particular first name. Use wildcards if you are unsure of the spelling.
Default	Blank (finds users with any first name)

Department	
Description	Use this field to find users that belong to a particular department. Use wildcard characters if you are unsure of the exact name or spelling, or if you want to find users in a number of similarly named departments.
Default	Blank (finds users in any department)

Extension Number (DN)	
Description	Use this field if you want to find users with a particular primary extension DN. Use wildcards to find users within a range of DNs.
Default	Blank (finds users with any extension DN)

Personal Verification Status	
Description	Use this field to find users who do not have, or have, a recorded personal verification.
Default	Any
Valid Options	Any, Not Recorded, Recorded

User Type	
Description	Use this field to find either temporary users or permanent users.
Default	Any
Valid Options	Any, Permanent, Temporary

Wildcard characters

Introduction

You can use wildcards in most of the fields in the Find Remote Voice Users screen in order to find a subset of users.

Definition: wildcard

A wildcard is a character that is used in a search string to represent an unknown or variable character or string of characters.

Types of wildcards

There are two wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.

Where you can use wildcards

You can enter wildcards in the following fields:

- Mailbox Number
- Last Name
- First Name
- Department
- Extension Number (DN)

Examples

The following examples show how wildcards can be used to find a range of users.

You enter	Result
"6321210_" in the Mailbox Number field (6321 is the ESN prefix of the remote site).	All mailboxes in the range 63212100 to 63212109 are found.
"7_99" in the Extension Number field.	Users with the following extension DNs are found: 7099, 7199, 7299, 7399, 7499, 7599, 7699, 7799, 7899, 7999.
"3213+" in the Mailbox Number field.	All mailboxes beginning with 3213 are found.
"+Engineering" in the Department field.	Users belonging to all engineering departments are found (such as Software Engineering, Hardware Engineering, Information Engineering).

Finding, listing, and printing remote voice users

Purpose

Use the find function to

- list (on screen) or print the found users
- view or modify any of the found users
- delete any of the found users

Administration level

Finding, listing, and printing remote voice users can be done only from the Customer Administration level.

Specifying search criteria

You only need to change a field if that field is part of your search criteria. All other fields should be left so that they display their default setting (blank or Any).

Network format

The mailbox numbers and DNs that are listed or printed are displayed in network format.

This means that any necessary network prefixes or steering codes are included as part of the DN or mailbox number.

Examples

If the dialing plan is ESN, you would see DNs like 62334433 where 6233 is the ESN prefix of the remote site and 4433 is the local DN.

If the dialing plan is CDP, you would see DNs like 54433, where 54 is the steering code of the site to which the user belongs.

Administration level

The Find function works only within a single customer group. It cannot find users throughout the entire Meridian Mail system.

Examples of use

Here are some examples of how you can use the Find function. You can

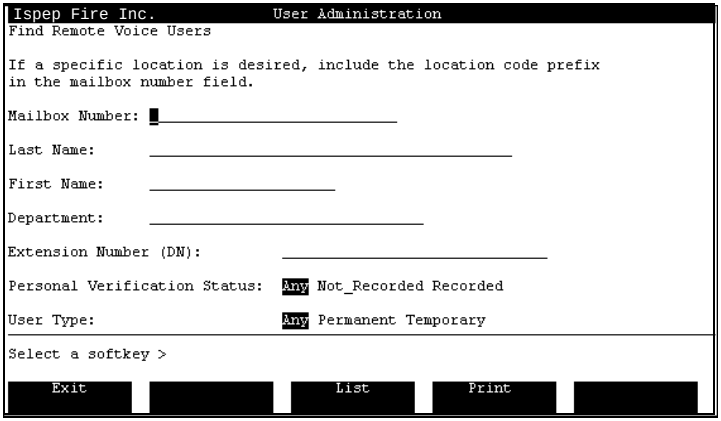
- find Cameron in the Technology department
- find an employee by last name only when you are not sure whether they go under Elizabeth, Liz, Betty or Beth as a first name
- find any users who have not yet recorded a personal verification
- find all users in the Documentation department, so that they can be reassigned to the new Information Products department

Procedure

To find a remote voice user (or subset of users), follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Find] softkey. **Result:** The Find Remote Voice Users screen is displayed.



4	Fill in the necessary fields in order to define your search criteria. **Note:** Field descriptions begin on page 10-29.

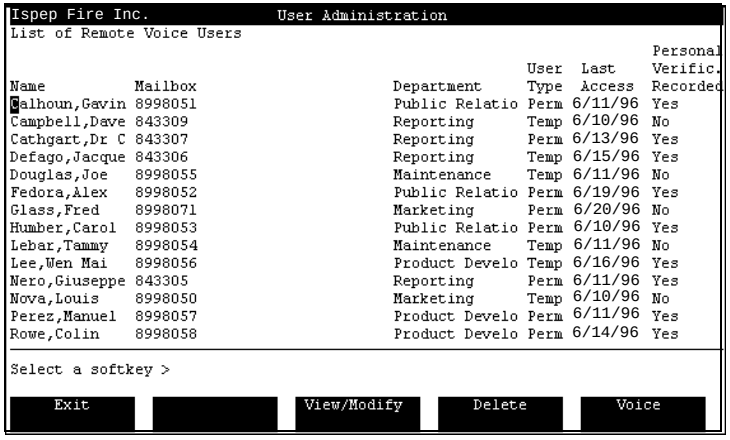
Step	Action

5 List or print the users that match the search criteria.

IF you want to	THEN
list the users that match the search criteria	go to step 6.
print the users that match the search criteria	go to step 9.
cancel the search	press [Exit].

6 Press the [List] softkey.

Result: The List of Remote Voice Users screen is displayed.



```
Ispep Fire Inc.              User Administration
List of Remote Voice Users

                                                                    Personal
                                                          User  Last    Verific.
Name           Mailbox                 Department         Type  Access  Recorded
Calhoun,Gavin  8998051                 Public Relatio     Perm  6/11/96  Yes
Campbell,Dave  843309                  Reporting          Temp  6/10/96  No
Cathgart,Dr C  843307                  Reporting          Perm  6/13/96  Yes
Defago,Jacque  843306                  Reporting          Temp  6/15/96  Yes
Douglas,Joe    8998055                 Maintenance        Temp  6/11/96  No
Fedora,Alex    8998052                 Public Relatio     Perm  6/19/96  Yes
Glass,Fred     8998071                 Marketing          Perm  6/20/96  No
Humber,Carol   8998053                 Public Relatio     Perm  6/10/96  Yes
Lebar,Tammy    8998054                 Maintenance        Temp  6/11/96  No
Lee,Wen Mai    8998056                 Product Develo     Temp  6/16/96  Yes
Nero,Giuseppe  843305                  Reporting          Perm  6/11/96  Yes
Nova,Louis     8998050                 Marketing          Temp  6/10/96  No
Perez,Manuel   8998057                 Product Develo     Perm  6/11/96  Yes
Rowe,Colin     8998058                 Product Develo     Perm  6/14/96  Yes

Select a softkey >

 Exit |  | View/Modify | Delete | Voice
```

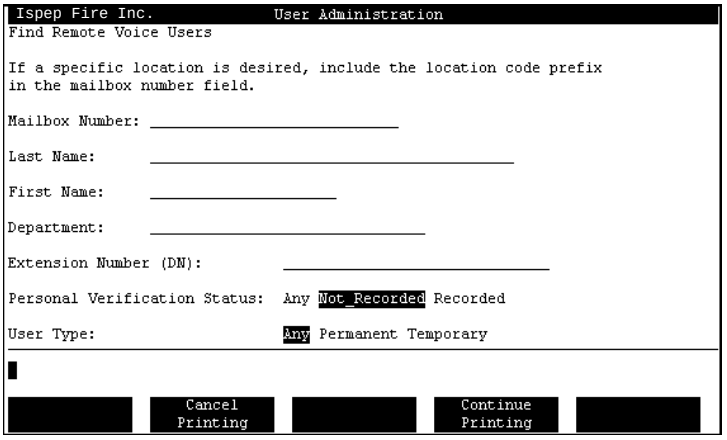
7 Do you want to view, modify, or delete a local voice user or record a personal verification?

- If yes, go to step 8.
- If no, press [Exit] to return to the Find Remote Voice Users screen.

8 Select the user by moving your cursor to the user's name and pressing the Spacebar.

IF you want to	THEN press	AND go to
view or modify a user	[View/Modify]	page 10-40.
delete a user	[Delete]	page 10-45.
record a personal verification for the user	[Voice]	page 10-19.

Step	Action
9	Press the [Print] softkey. **Result:** The Printing softkeys are displayed.



10	Do you want to continue printing? • If yes, press the [Continue Printing] softkey. **Note:** Once printing has started, you can stop it at any time by pressing the [Cancel Printing] softkey. • If no, press the [Cancel Printing] softkey.

Section D: Modifying and deleting remote voice users

In this section

Viewing and modifying remote voice users	10-40
Manually deleting remote voice users	10-45
How temporary remote voice users are automatically deleted from the system	10-49

Viewing and modifying remote voice users

Introduction

You may or may not know the mailbox number of the user you want to view or modify. Use this table to decide which procedure to follow to access the View/Modify Remote Voice User screen.

IF you	THEN follow
know the user's mailbox number	the procedure on this page.
do not know the users's mailbox number	the procedure on page 10-41.

Administration level

Viewing and modifying remote voice users can be done only from the Customer Administration level.

When to use

Use this procedure when you need to

- modify user information (such as last name or department)
- make a temporary user permanent
- make a permanent user temporary

Accessing the screen when you know the mailbox number

To access the View/Modify Remote Voice User screen directly, follow these steps.

Starting Point: The Customer Administration Menu

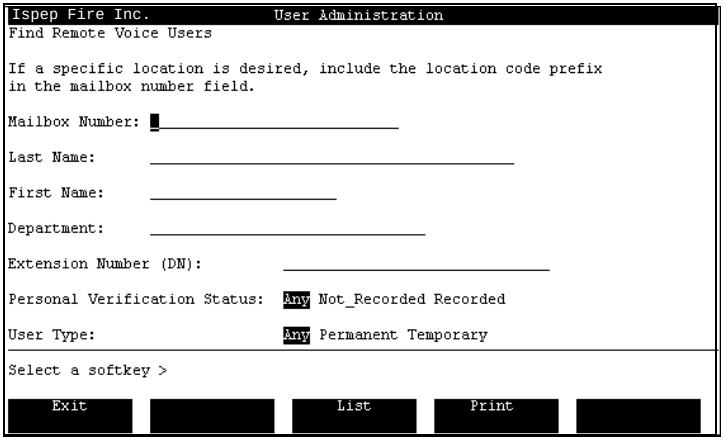
Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the user's mailbox number (including the access code and network prefix) and press Return. **Result:** The View/Modify Remote Voice User screen is displayed. See page 10-43.

Finding a remote voice user and accessing the screen

To find the remote voice user you want to modify when you do not know the mailbox number, follow these steps.

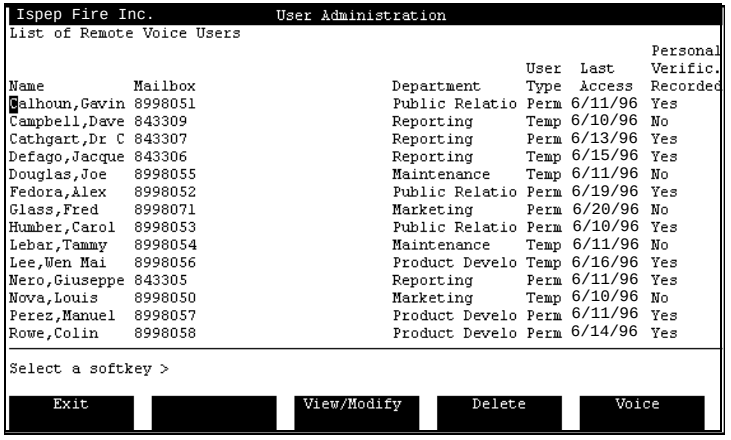
Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press [Find]. **Result:** The Find Remote Voice Users screen is displayed.



4	Enter the information you know about the user. **Examples:** Last Name, First Name, Department If you are not sure of your information, or want to see all the remote voice users listed, go to step 5.

Step	Action
5	Press [List]. **Result:** The List of Remote Voice Users screen is displayed.

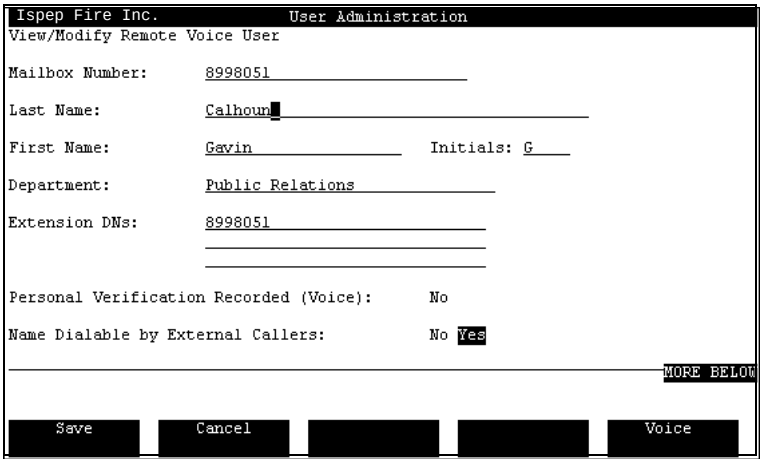

Ispep Fire Inc. User Administration
List of Remote Voice Users
Name Mailbox Department User Type Last Access Personal Verific. Recorded
Calhoun,Gavin 8998051 Public Relatio Perm 6/11/96 Yes
Campbell,Dave 843309 Reporting Temp 6/10/96 No
Cathgart,Dr C 843307 Reporting Perm 6/13/96 Yes
Defago,Jacque 843306 Reporting Temp 6/15/96 Yes
Douglas,Joe 8998055 Maintenance Temp 6/11/96 No
Fedora,Alex 8998052 Public Relatio Perm 6/19/96 Yes
Glass,Fred 8998071 Marketing Perm 6/20/96 No
Humber,Carol 8998053 Public Relatio Perm 6/10/96 Yes
Lebar,Tammy 8998054 Maintenance Temp 6/11/96 No
Lee,Wen Mai 8998056 Product Develo Temp 6/16/96 Yes
Nero,Giuseppe 843305 Reporting Perm 6/11/96 Yes
Nova,Louis 8998050 Marketing Temp 6/10/96 No
Perez,Manuel 8998057 Product Develo Perm 6/11/96 Yes
Rowe,Colin 8998058 Product Develo Perm 6/14/96 Yes
Select a softkey >
Exit
View/Modify
Delete
Voice

6	If you do not see the user you are looking for, scroll down using the down arrow key or the Page Down key to see more users.
7	Select the user you want to view or modify by moving your cursor to the user's name and pressing the Spacebar.
8	Press [View/Modify]. **Result:** The View/Modify Remote Voice User screen is displayed. See page 10-43.

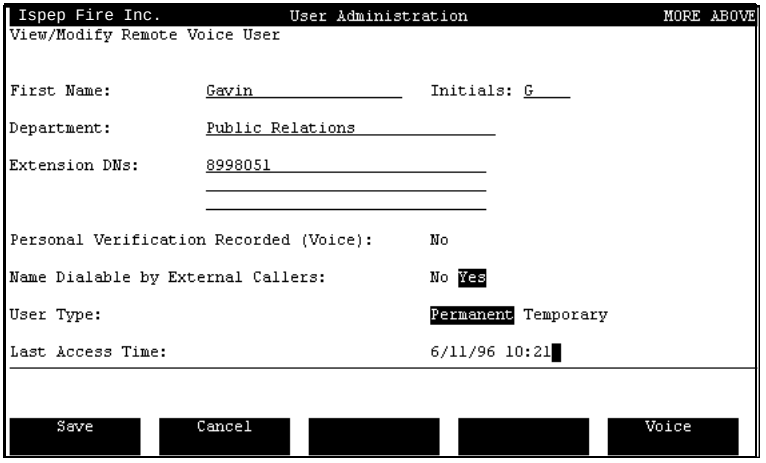
The View/Modify Remote Voice User screen

This is the View/Modify Remote Voice User screen.

Part 1



Part 2



Field descriptions

The fields in this screen are the same as in the Add Remote Voice User screen. For field descriptions, see “The Add Remote Voice User screen” on page 10-12.

Procedure

To view or modify a remote voice user, follow these steps.

Starting Point: The View/Modify Remote Voice User screen

Step	Action
1	Change the user's last name if necessary.
2	Change the user's department if necessary.
3	Change the extension DNs associated with the user if necessary.
4	Do you want to record a personal verification for the user? • If yes, see "Recording a personal verification for a remote voice user" on page 10-19. • If no, go to step 5.
5	Do you want to allow name dialing by external callers? • If yes, select Yes in the Name Dialable by External Callers field. • If no, select No in the Name Dialable by External Callers field.
6	Change the user type if necessary.
7	Do you want to save the user with the current information? • If yes, press [Save]. • If no, press [Cancel] or make any necessary changes and press [Save].

IF you want to	THEN select
make a temporary user permanent	Permanent in the User Type field.
make a permanent user temporary	Temporary in the User Type field.

Manually deleting remote voice users

Introduction

You may or may not know the mailbox number of the user you want to delete. Use this table to decide which procedure to follow to access the Delete Remote Voice User screen and then delete a user.

IF you	THEN follow
know the user's mailbox number	the procedure on this page.
do not know the users's mailbox number	the procedure on page 10-46.

Administration level

Manual deletion of remote voice users can be done only from the Customer Administration level.

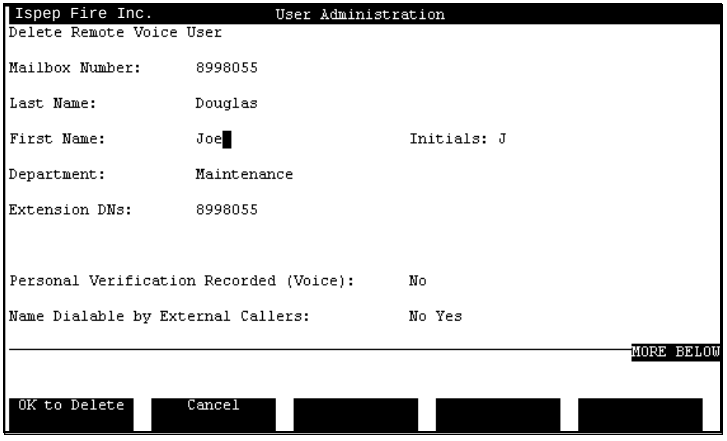
Deleting a user when you know the mailbox number

To access the Delete Remote Voice User screen directly, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Delete] softkey. **Result:** You are prompted for a mailbox number.

Step	Action
4	Enter the user's mailbox number (including the access code and network prefix) and press Return. **Result:** The Delete Remote Voice User screen is displayed.



5	Is this the user you want to delete? • If yes, go to step 6. • If no, press [Cancel]. Obtain the correct mailbox number or use the next procedure on page 10-46 to find the user.
6	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.
7	Do you want to delete another remote voice user? • If yes, repeat steps 4 to 6 until you have deleted all remote voice users that you need to delete at this time. • If no, press the [Cancel] softkey.

Deleting a remote voice user when you do not know the mailbox number

To find the remote voice user you want to delete when you do not know the mailbox number, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.

Step	Action
3	Press [Find]. **Result:** The Find Remote Voice Users screen is displayed.

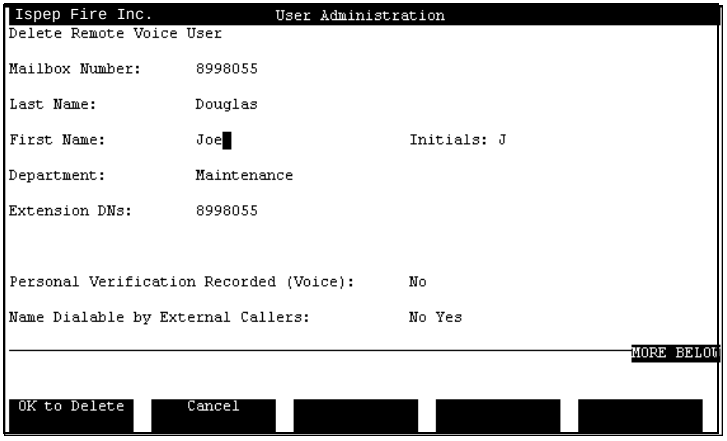
```
Ispep Fire Inc.              User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ______________________________________

First Name:     ____________________

Department:     ___________________________

Extension Number (DN):      ___________________________

Personal Verification Status:  Any Not_Recorded Recorded

User Type:                     Any Permanent Temporary

Select a softkey >

 Exit |      | List | Print |
```

Step	Action
4	Enter the information you know about the user. **Examples:** Last Name, First Name, Department If you are not sure of your information, or want to see all the remote voice users listed, go to step 5.
5	Press [List]. **Result:** The List of Remote Voice Users screen is displayed.

```
Ispep Fire Inc.              User Administration
List of Remote Voice Users

                                                                 Personal
                                                  User  Last     Verific.
Name          Mailbox                Department   Type  Access   Recorded
Calhoun,Gavin 8998051                Public Relatio Perm 6/11/96  Yes
Campbell,Dave 843309                 Reporting      Temp 6/10/96  No
Cathgart,Dr C 843307                 Reporting      Perm 6/13/96  Yes
Defago,Jacque 843306                 Reporting      Temp 6/15/96  Yes
Douglas,Joe   8998055                Maintenance    Temp 6/11/96  No
Fedora,Alex   8998052                Public Relatio Perm 6/19/96  Yes
Glass,Fred    8998071                Marketing      Perm 6/20/96  No
Humber,Carol  8998053                Public Relatio Perm 6/10/96  Yes
Lebar,Tammy   8998054                Maintenance    Temp 6/11/96  No
Lee,Wen Mai   8998056                Product Develo Temp 6/16/96  Yes
Nero,Giuseppe 843305                 Reporting      Perm 6/11/96  Yes
Nova,Louis    8998050                Marketing      Temp 6/10/96  No
Perez,Manuel  8998057                Product Develo Perm 6/11/96  Yes
Rowe,Colin    8998058                Product Develo Perm 6/14/96  Yes

Select a softkey >

 Exit |      | View/Modify | Delete | Voice
```

Step	Action
6	Select the user you want to delete by moving your cursor to the user's name and pressing the Spacebar.

Step	Action
7	Press [Delete]. **Result:** The Delete Remote Voice User screen is displayed.



8	Is this the user you want to delete? • If yes, go to step 9. • If no, press [Cancel].
9	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.

How temporary remote voice users are automatically deleted from the system

Introduction

Temporary remote voice users are automatically deleted by the system during nightly audits.

Timestamps

When a temporary remote voice user is added, the date and time at which the user was added is recorded. This is the timestamp.

When the timestamp is updated

This timestamp is updated whenever

- the user is modified via User Administration
- an Enterprise Networking message is received from the remote voice user
- a remote voice user's personal verification or mailbox number (when no verification is recorded) is played

The remote notification is played whenever

- the header of a message from the remote voice user is played
- a message is composed to the remote voice user
- the envelope of a message received from a remote voice user is played (when the local user presses 7-2)
- the remote voice user is name-dialed or name-addressed
- the recipient of a network message uses call sender to call the remote voice user back

Where timestamp information is displayed

The timestamp is displayed in the View/Modify Remote Voice User screen and the List of Remote Voice Users screen in the Last Access Time field.

The cutoff limit

There is a maximum number of temporary remote voice users that can be added to the system. Up to 1000 temporary remote voice users can be added to 1 and 2 node systems. For systems that have 3 or more nodes, up to 10 000 temporary remote voice users can be added. This value can be modified in the Network Configuration screen. The default maximum is 1000.

Whenever the total number of temporary remote voice users exceeds 75% of the cutoff limit, the nightly audit is run to delete some remote voice users.

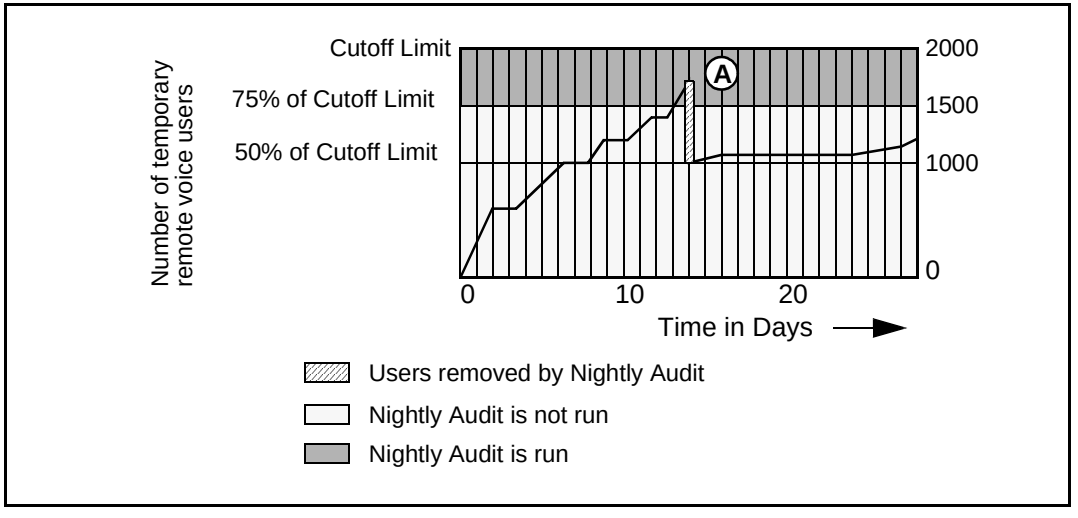
However, temporary remote voice users can still be added (using any method) up to the 100% mark. If this 100% limit is reached, no more remote voice users can be added to the system until after some temporary users are deleted by the audit.

The nightly audit

During the nightly audit, the least recently used users (those with the oldest timestamps) are deleted until the number of remaining temporary voice users equals 50% of the cutoff limit.

Example

The cutoff limit is 2000 temporary remote voice users. On the 14th day (as marked by point A), the number of temporary remote voice users reaches the 75% mark (1500). That night the nightly audit is run and the number of temporary remote voice users is reduced to 1000 (50%).



Chapter 11

Directory entry users

In this chapter

Overview	11-2
What is a directory entry user?	11-3
The Add Directory Entry User screen	11-4
Adding directory entry users	11-7
Recording a personal verification	11-8
The Find Directory Entry Users screen	11-10
Finding directory entry users	11-12
The List of Directory Entry Users screen	11-13
Printing directory entry users	11-15
Viewing or modifying directory entry users	11-16
Deleting directory entry users	11-18

Overview

Introduction

The User Administration screens provide the administrator with the facilities to add, find, view/modify, and delete directory entry users.

This chapter explains who directory entry users are and how to administer them.

User interface

Directory entry users are available in the VMUIF interface but lack name-dial capability (which is specific to the MMUI interface).

Administration level

You can administer directory entry users from the Customer Administration level only.

What is a directory entry user?

Concept

Directory entry users are users registered in the Meridian Mail directory who do not have mailboxes and, therefore, do not have access to voice messaging functions. They can, however, be referenced by such features as name dialing and automated attendant functions such as voice menus (if they are installed on your system).

Who should be a directory entry user

There are several reasons why users might not have a mailbox associated with their extensions.

- The user may not require or want a mailbox, or perhaps the user is not authorized to have a mailbox.
- Another common reason is that a user shares the same phone with other users. (In other words, you can associate a number of directory entry users with the same DN. This is unlike local voice users in that each local voice user must have a unique primary DN and mailbox number.)

Feature implications

Because directory entry users do not have mailboxes, they do not have access to voice messaging functions (such as compose and send) or other features such as Outcalling, AMIS Networking, and so on.

Directory entry users are included in the Meridian Mail directory. Therefore, you can dial those users using Thru-Dial features such as name dialing and automated attendant.

For example, if three people (say Tom, Dick, and Harriet) share the same phone, then another user can call Tom using the name dialing feature instead of dialing their extension number.

Similarly, an external caller can ring a directory entry user's phone through a voice menu or automated attendant. If the external caller does not remember Tom's extension, the caller can still dial the phone by entering Tom's name.

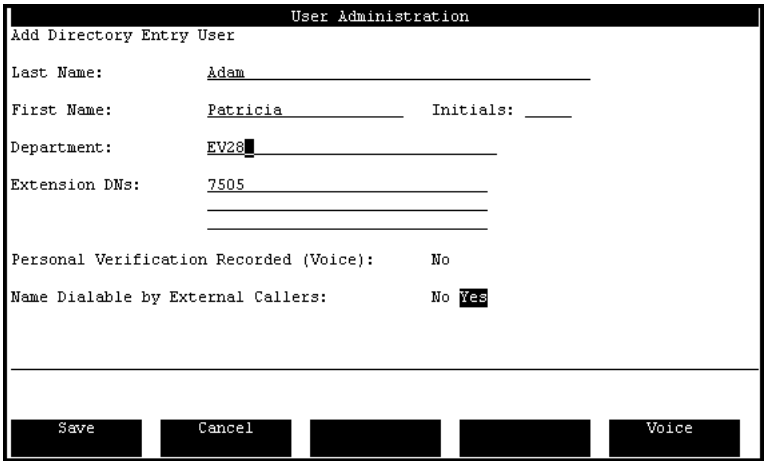
The Add Directory Entry User screen

Introduction

You may add directory entry users through the Add Directory Entry User screen.

The screen

Following is an example of the Add Directory Entry User screen.



Field descriptions

The following table describes the fields in the Add Directory User screen.

Last Name	
Description	This is the last name of the directory entry user. Be sure to fill in this field and ensure correct spelling because the name dialing feature uses this information.
Default	Blank
Maximum length	41 alphanumeric characters
Special characters	This field accepts any characters with the exception of the restricted characters “+”, “#”, and “?”. You should limit yourself to alphanumeric characters for name dialing to work properly.

First Name	
Description	This is the first name of the directory entry user.
Default	Blank
Maximum length	21 alphanumeric characters
Special characters	Same as Last Name

Initials	
Description	These are the initials of the directory entry user. You may use initials to distinguish users with identical first and last names. These initials, however, cannot be used in name dialing. If you do not enter any initials, the system will automatically fill in this field with the first initial of the user's first name.
Maximum length	5 alphanumeric characters

Department	
Description	This is the department of the directory entry user. You can retrieve users on the basis of their department when using the Find Directory Entry Users function (described later in this chapter). Only the first 26 characters of the department are displayed in the List of Directory Entry Users screen. Therefore, make sure that department names are unique based on the first 26 characters of their names.
Note	This field is not available in the VMUIF interface.
Default	Initially blank. After the first user, this field defaults to the department entered for the last user added.
Maximum length	31 alphanumeric characters
Special characters	Same as Last Name

Extension DNs

Description: This is the user's extension number(s). A user can be associated with up to three extensions.

Default: This field defaults to the primary extension.

> **ATTENTION**
>
> Make sure that none of these DNs conflict with any distribution list numbers. If a distribution list and a directory entry user share the same number, the distribution list number will take precedence over a directory entry user number during compose. The message will not be sent to the directory entry user.

Personal Verification Recorded (Voice)

Description: If a personal verification has been recorded for this user, this field displays Yes. No indicates that no verification is currently recorded. The setting in this field changes when the [Voice] softkey is used to record a verification.

The personal verification is played when the user's phone is dialed using Thru-Dial service (including name dialing). It informs callers that they have reached the correct phone.

Name Dialable by External Callers

Description: When the field is set to Yes, external callers can reach the user through the name dialing feature. This may occur when a caller reaches a voice menu and is prompted to enter an extension or the name of the person they want to speak to. (Internal callers can always use name dialing to call directory entry users.)

Note: This field is not available in the VMUIF interface.

Default: Yes

Adding directory entry users

Introduction Use the following procedure to add new directory entry users.

Up to three extensions Like local voice users, each directory entry user can be associated with up to three different extensions. Primary extension numbers do not have to be unique. A number of users can share the same extension.

Procedure To add a new directory entry user, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Press the [Add] softkey.
4	Enter the extension number and press <Return>.
5	Enter the Last Name of the new user.
6	Enter the First Name of the new user.
7	If the interface is MMUI, enter the Department of the new user.
8	Enter the Extension Number(s) of the new user.
9	Do you want to record a personal verification? • If yes, see “Recording a personal verification” on page 11-8. • If no, go to step 10.
10	If the interface is MMUI, do you want external callers to be able to name dial this user? • If yes, set the Name dialable by external callers field to Yes. • If no, set the Name dialable by external callers field to No.
11	Do you want to save the user? • If yes, press [Save]. • If no, press [Cancel].

Recording a personal verification

Introduction

The administrator can use this procedure to record a personal verification on behalf of a directory entry user.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Directory Entry User screen, or the View/ Modify Directory Entry User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey.
3	Enter the extension of the phone you will use to record the verification and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.
5	Press the [Record] softkey.
6	At the sound of the beep, speak the user's (and, optionally, the user's extension). **Example:** "Billy McGee at extension 8123."
7	Press the [Stop] key to stop recording.

Step	Action
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.
9	Do you want to rerecord the verification? • If yes, press the [Delete] softkey to delete the current recording and repeat steps 5 to 8. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.

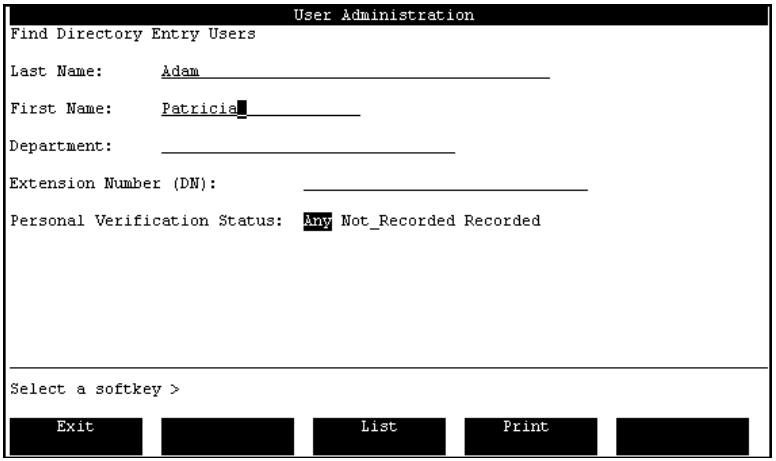
The Find Directory Entry Users screen

Introduction

You can locate a directory entry user by extension number or name using the Find function.

The screen

Following is an example of the Find Directory Entry Users screen.



Field descriptions

The following table describes the fields in the Find Directory Users screen.

Last Name	
Description	Fill in this field if you want to retrieve a particular user and remember only the last name. Use wildcard characters (“+”, “?”, and”_”) if you are unsure of the spelling.
First Name	
Description	Fill in this field if you want to retrieve a particular user and you remember only the first name. If you also know the last name, the first name will narrow the search (if a number of users have the same last name). Use wildcard characters (“+”, “?”, and”_”) if you are unsure of the spelling.

Department	
Description	This field can help you narrow down a search even further if, for example, you can remember only the first or last name of the user you want to find. You can also use this field if you want to retrieve all users that belong to a particular department. Use wildcard characters if you are unsure of the spelling or the exact name of the department.

Extension DNs	
Description	This is the user's primary extension DN. Enter the user's DN if it is known. Use wildcard characters ("+", "?", and"_") to retrieve a subset of users in a particular range of DNs.

Personal Verification Recorded (Voice)	
Description	Set this field to Not_Recorded to retrieve all directory users who do not have a recorded personal verification. Since it is a good idea for all users to have a personal verification, you should record a verification for the user. If the personal verification status is not important, make sure that this field is set to Any (the default).

Finding directory entry users

Introduction

The [Find] softkey can be used to search for a directory entry user, depending upon your search parameters.

Procedure

To access the Find Directory Entry User screen, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Press the [Find] softkey. **Result:** The Find Directory Entry User screen is displayed.

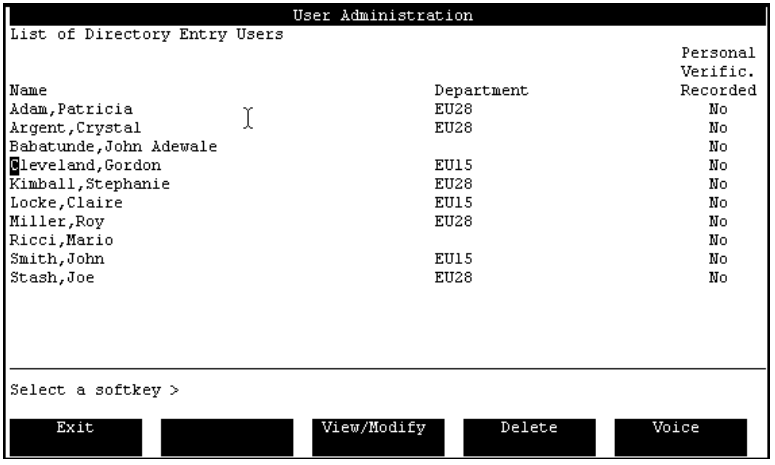
The List of Directory Entry Users screen

Introduction

The List of Directory Entry Users screen appears when the [List] softkey on the Find Directory Entry Users screen is used. It provides a list of user names matching the search parameters entered in the Find Directory Entry Users screen.

Screen

Following is an example of the List of Directory Entry Users screen.



Field descriptions

The following table describes the fields in the List of Directory Entry Users screen.

Name	
Description	This is the user's last name followed by the first name.
Department	
Description	This is the name of the department to which the user belongs.
Personal Verific. Recorded	
Description	This field indicates whether or not a spoken name (personal verification) has been recorded for this user.

Viewing a list of directory entry users

To view a list of directory entry users from your search, follow this procedure.

Starting Point: The Find Directory Entry Users screen

Step	Action
1	Fill in the screen with the required search parameters.
2	Press [List] to display the results of the search on the screen.
3	To view or modify a directory entry user, move to the user's line and press the <spacebar> to select it.

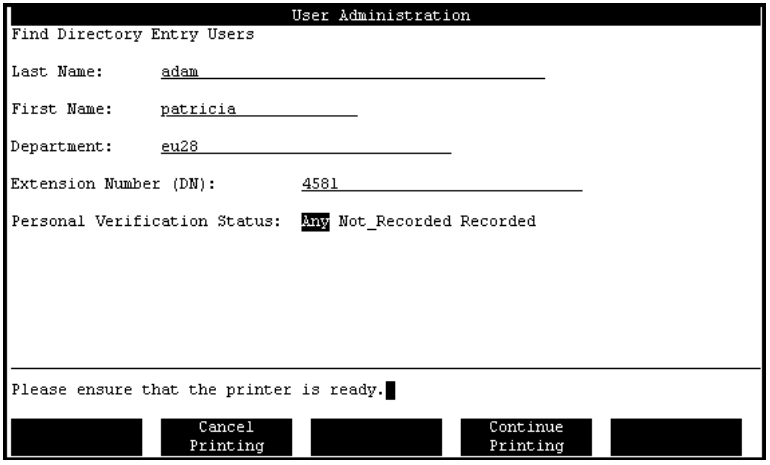
Printing directory entry users

Introduction

The results of your search for an individual or list of directory entry users can also be printed. Instead of using the [List] softkey on the Find Directory Entry Users screen, use the [Print] softkey.

Screen

Following is an example of the Find Directory Entry Users screen, after being filled out for an individual user.



Procedure

To print out a list of directory entry users from your search, follow this procedure.

Starting Point: The Find Directory Entry Users screen

Step	Action
1	Do you want to print a list of all directory entry users? • If yes, leave all fields blank. • If no, fill in the screen with the required search parameters.
2	Press the [Print] softkey.
3	Ensure the printer is working and press the [Continue Printing] softkey.

Viewing or modifying directory entry users

Introduction

This procedure explains how to view or modify a directory entry user. Initially, you are prompted for an extension number.

WHEN	THEN
more than one directory entry user is associated with that extension	you will see the List of Directory Entry Users screen (see page 11-13).
only one directory entry user is associated with the extension	the View/Modify Directory Entry User screen is displayed.

Field descriptions

The fields in the View/Modify Directory Entry User screen are identical to those on the Add Directory Entry User screen, described on page 11-4.

Procedure

To view or modify a directory entry user, follow this procedure.

Starting Point: The Customer Administration Menu

Step	Action
1	Choose User Administration
2	Choose Directory Entry User.
3	Do you know the user's extension number? • If yes, press the [View/Modify] softkey. Go to step 4. • If no, press, the [Find] softkey.
4	Enter the extension number.

IF	THEN
more than one user shares the extension only	the List of Directory Entry Users screen appears. Go to step 5.
one user is assigned to the extension number	the View/Modify Directory Entry User screen appears. Go to step 6.

Step	Action
5	Choose a user by placing the cursor on the user you want to view or modify. Press the <spacebar> to select the user and press [View/Modify].
6	Modify the fields as needed.
7	Do you want to record a personal verification? • If yes, go to “Recording a personal verification” on page 11-8. • If no, go to step 8.
8	Do you want to save the modified user? • If yes, press [Save]. **Result:** The system saves the modified directory entry user. You are prompted for another extension number. (Go to step 4 to modify another user.) • If no, press [Cancel]. **Result:** Any changes will be discarded. The Directory Entry User Administration softkeys screen or the List of Directory Entry Users screen is displayed.

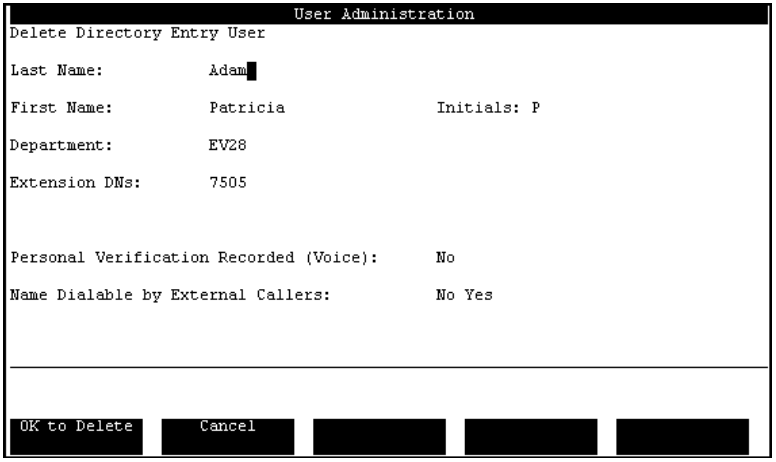
Deleting directory entry users

Introduction

This procedure explains how to delete a directory entry user.

The Delete Directory Enter User screen

Following is an example of the Delete Directory Entry User screen.



Procedure

To delete a directory entry user once you have selected the user from the list of users, follow this procedure.

Starting Point: The Customer Administration Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Do you know the user's extension DN? • If yes, press the [Delete] softkey and go to step 6. • If no, press the [Find] softkey. **Result:** The Find Directory Entry Users screen is displayed.

Step	Action
4	Enter the extension number.

IF	THEN
more than one user shares the extension only	the List of Directory Entry Users screen appears. Go to step 5.
one user is assigned to the extension number	the View/Modify Directory Entry Users screen appears. Go to step 6.

5	Choose a user by placing the cursor on the user you want to delete. Press the <spacebar> to select the user and press [Delete].
6	Do you want to delete the user? • If yes, press [OK to Delete]. • If no, press [Cancel].

Chapter 12

Distribution lists

In this chapter

Overview	12-2
Understanding distribution lists	12-3
Limitations on distribution lists	12-4
Accessing the Distribution Lists softkeys screen	12-7
Adding a customer distribution list	12-9
Finding and viewing a customer distribution list	12-16
Modifying a customer distribution list	12-21
Printing a customer distribution list	12-23
Deleting a customer distribution list	12-25

Overview

Introduction

This chapter provides an overview of distribution lists. It explains what a distribution list is and briefly sets out the differences between customer and personal distribution lists.

It also provides information and procedures for administering customer distribution lists:

- adding a customer distribution list
- finding an existing customer distribution list
- viewing a customer distribution list
- modifying a customer distribution list
- printing a customer distribution list
- deleting a customer distribution list

Administration level

You can administer distribution lists from the Customer Administration level only.

Understanding distribution lists

Introduction

A distribution list is a mailing list that enables you to send the same message to a number of people. After you add and save a distribution list, you can reuse it whenever you need to send messages to the same group or groups of people.

Adding a distribution list involves assigning a unique number and title to the list and specifying the mailbox numbers that you want to include on it. If you choose to, you can also make a voice recording of the list's title.

When you compose a message, you specify the distribution list number as you would any other mailbox number. Then when you send your message, it is deposited in every mailbox included in the list.

There are two types of distribution lists: customer distribution lists and personal distribution lists.

This chapter contains information about administering customer distribution lists. Personal distribution lists are explained in the *Meridian Mail Voice Messaging User Guide* (PO 839942).

Definition: customer distribution list

You add a customer distribution list through Meridian Mail User Administration.

You can add any number of customer distribution lists, each containing up to 120 entries.

Definition: personal distribution list

Meridian Mail users create personal distribution lists from their telephone sets.

A user can create up to 9 personal distribution lists, each containing up to 99 entries.

Limitations on distribution lists

Introduction

This topic presents an overview of factors that affect the creation and use of distribution lists.

Message number and size

The number of addresses to which a user can successfully send a message simultaneously depends on the size of the message, as shown in the following table.

Length of message	Number of addresses
90 minutes voice	up to 290 addresses
60 minutes voice	up to 350 addresses
10 minutes voice	up to 425 addresses
1 minute voice	up to 440 addresses

Note: Each customer distribution list is one address, regardless of the number of entries on the list, while each entry on a personal distribution list is one address. Therefore, a customer distribution list with 10 entries is 1 address, while a personal distribution list with 10 entries is 10 addresses.

Restrictions on distribution list numbers

The following restrictions are placed on distribution list numbers:

- A system distribution list cannot be assigned a number between 1 and 9. These numbers are reserved for personal distribution lists.
- Each distribution list must have a unique distribution list number.
- A distribution list number must not conflict with any dialing plan prefixes or codes. (These are explained further in the description of the List Number field on page 12-11.) This includes the Network Wide Broadcast Prefix, defined in the Network Configuration screen.
- A distribution list number cannot be the same as any mailbox number, including the broadcast mailbox number. The default broadcast mailbox number is 5555.

- A distribution list number cannot share a directory entry user's DN. If a distribution list number and a directory entry user number are the same, the distribution list number takes precedence over the directory entry user number when a list is composed.

MMUI restrictions

Distribution lists can include the following types of numbers:

- mailbox numbers of local voice users
- mailbox numbers of remote voice users
- broadcast mailbox numbers for particular Networking sites (personal distribution lists only)

To include a mailbox number at an AMIS site, you must have Meridian Networking installed. You must also define the AMIS site as a virtual node in the Meridian network. For more information, refer to the *Virtual Node AMIS Installation and Administration Guide* (NTP 555-7001-245).

To include individual users at remote sites in a Meridian network, you must define them as remote voice users in the local database.

The following types of numbers do not have mailboxes associated with them and, therefore, cannot be included in a distribution list:

- numbers of directory entry users
- remote notification targets
- delivery to non-user targets

Restrictions on personal distribution lists

A personal distribution list can contain up to 99 entries. There are, however, some limitations on the total number of addresses to which an outgoing message can be sent using personal distribution lists. If a user tries to send a message to a number of distribution lists, he or she may get the following message if the maximum address size of the message is exceeded: *"Your command cannot be completed at this time. Please try again, or contact your administrator."* The message is deleted, and the user is positioned at the next message in the mailbox (or at the end of the mailbox) and can use other commands normally.

Note: If VMUIF is installed and you want VMUIF subscribers to be able to address messages to personal distribution lists, you must define a personal distribution list prefix in the Voice Messaging Options screen. By default, no prefix is defined.

Accessing the Distribution Lists softkeys screen

Introduction

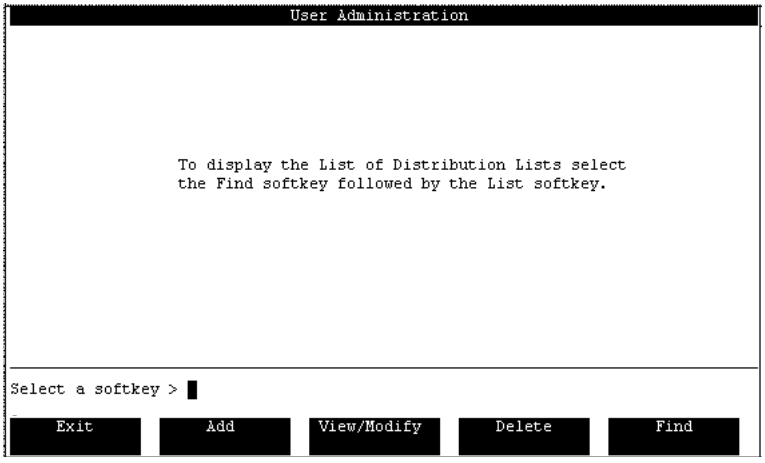
Many of the administration tasks concerned with distribution lists begin with the Distribution Lists softkeys screen. These tasks include the following:

- adding a distribution list by using the [Add] softkey
- adding mailboxes to or removing mailboxes from an existing distribution list by using the [View/Modify] softkey
- deleting a distribution list by using the [Delete] softkey
- finding a distribution list by using the [Find] softkey followed by the [List] softkey

This topic explains how to get to the Distribution Lists screen.

The Distribution Lists softkeys screen

The following shows an example of the Distribution Lists softkeys screen.



Procedure

To go to the Distribution Lists softkeys screen, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select User Administration.
2	Select Distribution Lists. **Result:** The system displays the Distribution Lists softkeys screen.

Adding a customer distribution list

Introduction

You add a distribution list using the Add Distribution List screen. Adding a distribution list involves assigning a unique number and title to the list and specifying the mailbox numbers that you want to include on it. If you choose to, you can also make a voice recording of the list's title.

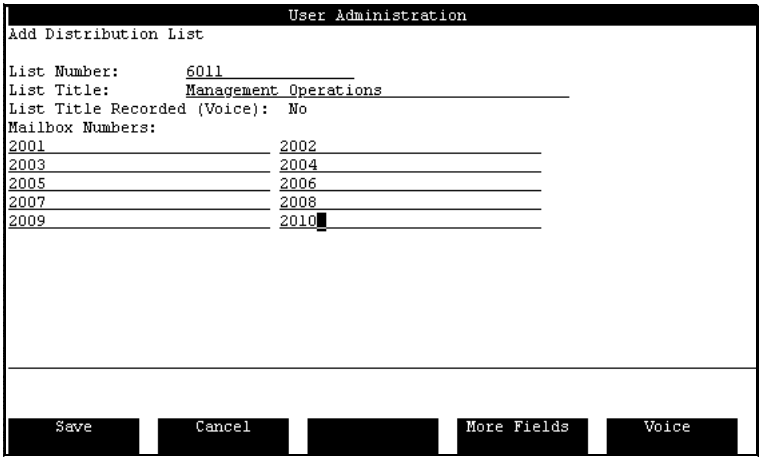
When you compose a message, you specify the distribution list number as you would any other mailbox number. Then when you send your message, it is deposited in every mailbox included in the list.

If you assign numbers to distribution lists that are of a different length from those you use as mailbox numbers, you are able to avoid confusion or conflict with your mailbox numbers.

Although making a voice recording of the list title is optional, the voice recording has the same purpose as a personal verification. That is, it is played when a distribution list number is entered when addressing messages. The list title describes who is included in the list or the purpose of the list. This makes it easier to identify whether you have entered the correct list number when you address messages.

The Add Distribution List screen

The following shows an example of the Add Distribution List screen.



Field descriptions

The following table describes the fields in the Add Distribution List screen.

List Number	
Description	This value uniquely identifies the distribution list. The list number cannot be the same as the following numbers: • personal distribution list numbers The single digits 1 to 9 are reserved for personal distribution lists. • any mailbox number, including the broadcast mailbox number The default broadcast mailbox number is 5555. • a directory entry user's DN If a distribution list and a directory entry user share a number, the distribution list number takes precedence over the directory entry user number when a list is composed. • the name dialing prefix The default name dialing prefix is 11. Do not use 11 to number a list unless you have changed the name dialing prefix in the Voice Messaging Options screen. • the Delivery to Non-User prefix • another distribution list number • any dialing plan access code prefixes • the Network-Wide Broadcast prefix
Default	There is no default. You can use any valid number.
Valid range	from 10 to 999999999999999999 (there are 18 9s; only digits are allowed)

List Title	
Description	This is the title of the distribution list. It can be up to 41 characters in length. Do not use "?", "+", or "_" (underscore) which are wildcard characters. The title can be used to address the distribution list by name when you are composing and sending a message to mailboxes on the distribution list.
Default	There is no default value.
Valid range	There is no default range.

List Title Recorded (Voice)	
Description	This read-only field indicates whether a voice recording of the list title has been made. It is a good idea to record a title for each distribution list. This helps you to identify the list after you have entered its number when composing a message. Choose a name that uniquely identifies this list. This field changes only when you use the [Voice] softkey to record or delete a list title.
Default	No
Valid range	There is no default range.

Mailbox Numbers	
Description	In these fields, you type the mailbox numbers of the users you want to include on the distribution list. Mailbox numbers can be up to 18 digits in length. To add more mailbox fields, use the [More Fields] softkey.
Default	These fields are blank.
Valid range	from 10 to 999999999999999999 (there are 18 9s) ***Note:*** These must be valid local and remote voice users.

Adding a customer distribution list

To add a customer distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [Add] softkey. **Result:** The system prompts for a distribution list number.
2	Type a valid number. **Note:** For information about valid distribution list numbers, see the description of the List Number field on page 12-11. **Result:** The system displays the Add Distribution List screen.
3	Type a name for the list in the List Title field.
4	Type the mailbox numbers of the users you want to include in the distribution list. **Note:** If you are including the mailbox number of a remote voice user, type the network prefix (ESN prefix or CDP steering code), followed by the mailbox number. The system informs you if any of the numbers are not valid.
5	To add more mailboxes, use the [More Fields] softkey. **Note:** The system draws one row of fields each time you use this softkey. You can include up to 120 mailboxes in a system distribution list.
6	Make a voice recording of the title of the distribution list. **Note:** This step is optional. For more information, see “Recording a distribution list title” on page 12-14.

Step	Action
7	Use the following table to determine the next step.

IF you want to	THEN
save your distribution list	go to step 8.
add another distribution list	go to step 8.
exit without saving your distribution list	go to step 9.

Step	Action
8	To save your distribution list, use the [Save] softkey. **Result:** The system saves your distribution list. If your distribution list is long, it may take a few moments to save. The system then prompts you to enter a number for a new distribution list. To add another distribution list, type a valid number, and go to step 3. **Note:** For information about valid distribution list numbers, see the description of the List Number field on page 12-11.
9	To exit without saving your distribution list, use the [Cancel] softkey. **Result:** The system does not save the distribution list, and you are returned to the Distribution Lists softkeys screen.

Recording a distribution list title

To make a voice recording of the title of a distribution list, follow these steps.

Note: This procedure is optional.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
2	Type the number of the distribution list for which you are recording a title.
3	Select the [Voice] softkey. **Result:** The system prompts for an extension number.
4	Type the extension number of the telephone set you are going to use to record the title, and press <Return>. **Result:** The phone rings.

Step	Action
5	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
6	Select the [Record] softkey. **Result:** The system displays a message on the console requesting you to make the recording. The system displays the [Stop] softkey in place of the [Record] softkey. You hear a beep through the telephone receiver.
7	At the beep, say the list title into the telephone handset.
8	To stop recording, use the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
9	If you are satisfied with the recording, select either the [Disconnect] softkey or the [Return] softkey. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to type the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must again type the telephone extension.

Finding and viewing a customer distribution list

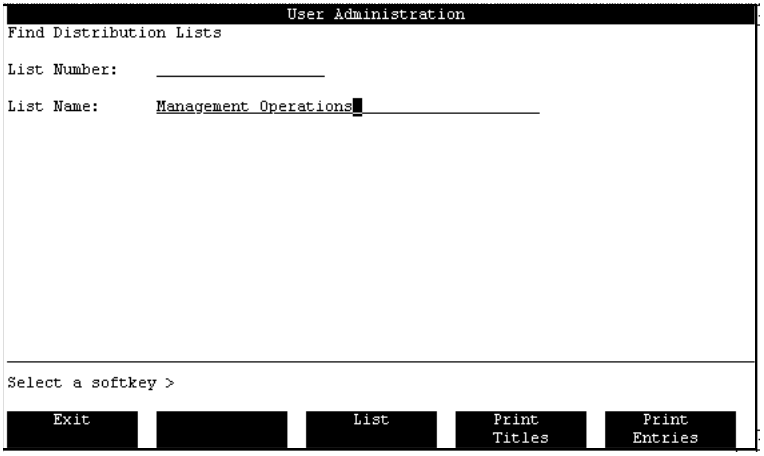
Introduction

The Find function generates a list of distribution lists. Use this function to locate a particular distribution list or a subset of lists.

Use the List function to view onscreen the distribution lists that you retrieve. You can then view, modify, or delete these distribution lists.

The Find Distribution Lists screen

The following shows an example of the Find Distribution Lists screen. In this example, the user is searching for a list by name.



Field descriptions

For explanations of the fields in the Find Distribution Lists screen, see “Field descriptions” on page 12-11.

The fields are identical to those in the Add Distribution List screen, except that you can use the wildcards “ +”, “_”, and “?” to retrieve subsets of lists.

Using wildcards

If you do not know the name or number of a list you want to retrieve but do not want to retrieve all available distribution lists, you can use wildcards to narrow your search.

Types of wildcards

There are three wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.
?	The question mark (?) produces a “sound match”. It finds distribution lists with names that sound alike.

Examples

The following examples show how wildcards can be used to find a subset of distribution lists.

You enter	Result
“2_” in the List Number field	All lists in the range 20 to 29 are found.
“3+” in the List Number field	All distribution lists beginning with 3 are found.
“+Engineering” in the List Name field	All distribution lists that end in “Engineering” are found (such as Software Engineering, Hardware Engineering, Information Engineering).
Braymore?	All distribution lists with names that sound like Braymore (Breymore, Braemore), are found.

Finding and viewing a distribution list

To find a distribution list or a subset of a distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [Find] softkey. **Result:** The system displays the Find Distribution Lists screen.
2	Use the following table to determine the next step.

IF you want to	THEN
find a distribution list	type the complete number or name of the list.
find a subset of a distribution list	use wildcard characters to create a search pattern. **Example:** To retrieve all lists beginning with 1, type **1+** in the List Number field. **Note:** For more information about wildcards, See “Using wildcards” on page 12-17.
retrieve a distribution list whose name you do not know	leave both fields blank.

3	To view a list of the retrieved distribution lists, use the [List] softkey. **Result:** The system displays the List of Distribution Lists screen. **Note:** The system displays only the first 20 characters of the name of each retrieved list.
4	Use the following table to determine the next step.

IF you want to	THEN
print the retrieved list title or list entries	go to step 5.
modify a retrieved list	see “Modifying a customer distribution list” on page 12-21.
delete a retrieved list	see “Deleting a customer distribution list” on page 12-25.

Step	Action
5	Use the [Print Titles] softkey or the [Print Entries] softkey, depending on what you want to print.

IF you want to print	THEN
the titles and list numbers only	select the [Print Titles] softkey.
the mailboxes associated with the retrieved list or lists	select the [Print Entries] softkey.

Result: The system displays the [Continue Printing] softkey and the [Cancel Printing] softkey.

It also prompts you to check that the printer is ready.

6 Use the following table to determine the next step.

IF you want to	THEN
print the list	go to step 7.
cancel printing	go to step 8.

7 Select the [Continue Printing] softkey.

Result: The system begins to print the distribution list titles or entries.

When printing is complete, the system again displays the Find Distribution Lists screen.

Note: To stop printing at any time, select [Cancel Printing].

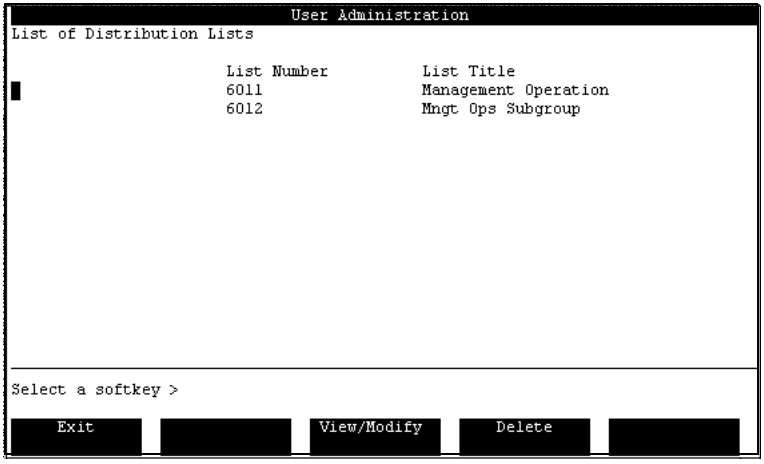
8 Select the [Cancel Printing] softkey.

Result: The system cancels the print operation, and you are returned to the List of Distribution Lists screen.

Note: There may be some delay before control is returned to the screen because the system waits for the printer to stop.

The List of Distribution Lists screen

The following shows an example of the List of Distribution Lists screen with two retrieved lists.



Field descriptions

For explanations of the fields in the List of Distribution Lists screen, see “Field descriptions” on page 12-11. The fields are identical to those in the Add Distribution List screen.

Modifying a customer distribution list

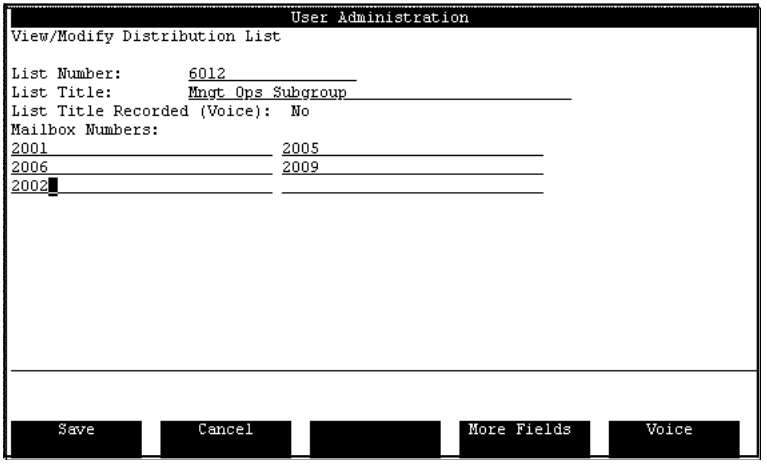
Introduction

This topic explains how to make changes to an existing distribution list. From the View/Modify Distribution List screen, you can add one or more mailbox numbers to a distribution list. You can change the mailboxes that you include on a list, or you can delete one or more mailboxes.

Note: To delete an entire distribution list, see "Deleting a customer distribution list" on page 12-25.

The View/Modify Distribution List screen

The following shows an example of the View/Modify Distribution List screen.



Field descriptions

For explanations of the fields in the View/Modify Distribution List screen, see "Field descriptions" on page 12-11. The fields are identical to those in the Add Distribution List screen.

Procedure

To modify a distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Do you know the number of the distribution list you want to modify? **IF** / **THEN** yes — go to step 2. no — see “Finding and viewing a customer distribution list” on page 12-16.
2	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
3	Type the number of the list you want to modify, and press <Return>. **Result:** The system displays the View/Modify Distribution List screen.
4	Make your changes to your list. **Note:** Use the [More Fields] softkey if you reach the last available mailbox number and wish to add more mailboxes to the list. You can include up to 120 mailboxes in a system distribution list.
5	Use the following table to determine the next step. **IF you want to** / **THEN** save your distribution list — go to step 6. exit without saving your distribution list — go to step 7.
6	To save your modified distribution list, use the [Save] softkey. **Result:** The system saves your changes. It then prompts you for another distribution list number. To modify another list, go to step 3.
7	To exit without saving your changes, use the [Cancel] softkey. **Result:** The system returns you to the Distribution Lists softkeys screen.

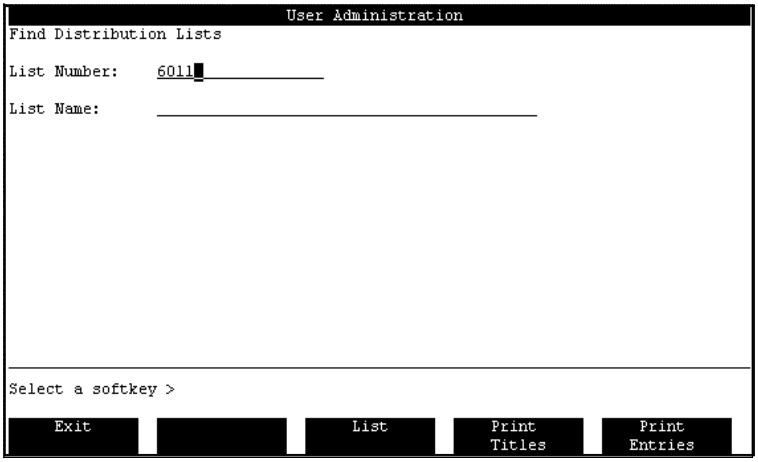
Printing a customer distribution list

Introduction

This topic explains how to print information in a customer distribution list using the softkeys in the Find Distribution Lists screen.

The Find Distribution Lists screen

The following shows the position of the print keys on the Find Distribution Lists screen.



Field descriptions

For explanations of the fields in the Find Distribution List screen, see “Field descriptions” on page 12-11. The fields are identical to those in the Add Distribution List screen.

Procedure

To print distribution list information, follow these steps.

Starting Point: The Find Distribution Lists screen

Step	Action
1	Use the [Print Titles] softkey or the [Print Entries] softkey, depending on what you want to print.

IF you want to print	THEN
the titles and list numbers only	select the [Print Titles] softkey.
the mailboxes associated with the retrieved list or lists	select the [Print Entries] softkey.

Result: The system displays the [Continue Printing] softkey and the [Cancel Printing] softkey.

It also prompts you to check that the printer is ready.

2 Use the following table to determine the next step.

IF you want to	THEN
print the list	go to step 3.
cancel printing	go to step 4.

3 Select the [Continue Printing] softkey.

Result: The system begins to print the distribution list titles or entries.

When printing is complete, the system again displays the Find Distribution Lists screen.

Note: To stop printing at any time, go to step 4.

4 Select the [Cancel Printing] softkey.

Result: The system cancels the print operation, and you are returned to the List of Distribution Lists screen.

Note: There may be some delay before control is returned to the screen because the system waits for the printer to stop.

Deleting a customer distribution list

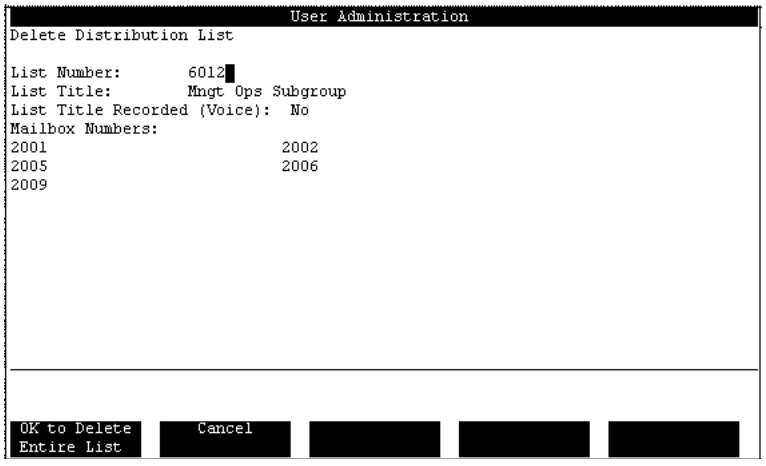
Introduction

This topic explains how to delete a customer distribution list using the Delete Distribution List screen. This screen enables you to view a distribution list before you delete it.

To delete mailbox numbers from a distribution list but not the entire list, see "Modifying a customer distribution list" on page 12-21.

The Delete Distribution List screen

The following shows an example of the Delete Distribution List screen.



Field descriptions

For explanations of the fields in the Delete Distribution List screen, see "Field descriptions" on page 12-11. The fields are identical to those in the Add Distribution List screen.

Note: In the Delete Distribution List screen, these fields are read-only.

Procedure

To delete a customer distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Do you know the number of the distribution list you want to delete?

IF	THEN
yes	go to step 2.
no	see “Finding and viewing a customer distribution list” on page 12-16.

Step	Action
2	Select the [Delete] softkey. **Result:** The system prompts for a distribution list number.
3	Type the number of the list you want to delete, and press <Return>. **Result:** The system displays the Delete Distribution List screen.
4	Use the following table to determine the next step.

IF you want to	THEN
delete your distribution list	go to step 5.
exit without deleting your distribution list	go to step 6.

Step	Action
5	To delete your distribution list, use the [Delete] softkey. **Note:** The system deletes the list. It then prompts you for another distribution list number. To delete another list, go to step 3.
6	To exit without deleting the list, use the [Cancel] softkey. **Result:** The system returns you to the Distribution Lists softkeys screen.

Chapter 13

General administration–an overview

In this chapter

General Administration 13-2

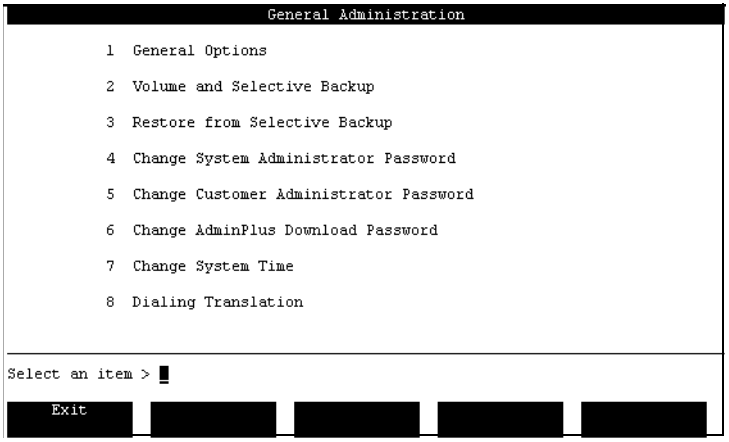
General Administration

Introduction

This chapter provides an overview of the General Administration menu and related screens. It also describes how General Administration tasks are split between System Administration and Customer Administration.

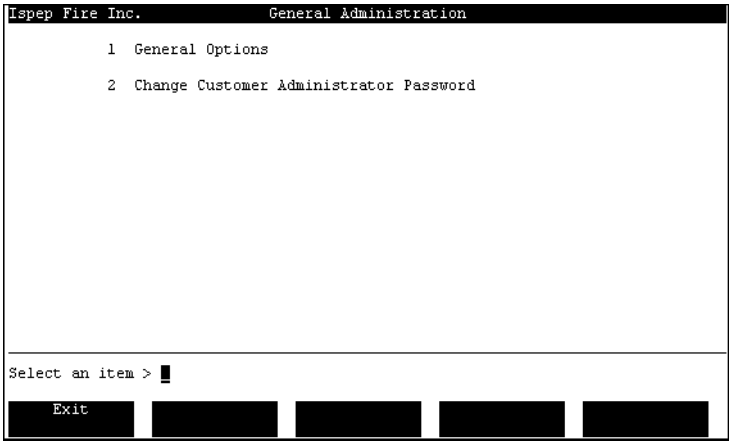
The menu: system administration

This is an example of the General Administration menu at the System Administration level.



The menu: customer administration

This is an example of the General Administration menu at the Customer Administration level.



General Options

The General Options screen is available from both System Administration and Customer Administration.

System administration

Some general options apply to the entire system. You can do the following at the System Administration level:

- modify the system name, system number, and system addressing lengths
- choose the ACCESS default customer number
- choose the Integrated Mailbox Administration default customer number
- view a list of installed features
- choose the date format for reports
- define the SEER printer and Reports printer port names

Customer administration

Other general options are specific to each customer group. You can do the following at the Customer Administration level:

- modify the customer name
- modify the customer type

- enable the following features (if installed) for each customer
  - Voice Menus and Announcements
  - Voice Forms
  - Fax on Demand
  - Meridian Mail Networking
- define the attendant DN
- assign up to 15 classes of service to each customer

Volume and Selective Backup

Administration level

You can back up and restore data from the System Administration level only.

Description

The Volume and Selective Backup option allows you to make backup copies of some or all of the data stored on your hard disk. You can perform the following types of backups:

- full backup to tape
- partial backup to tape or disk

Note: Partial backup to disk can only be done if the Disk-to-Disk Backup feature is installed.

- selective backup of users
- selective backup of services

Restore from Selective Backup

Administration level

You can restore from a selective backup from the System Administration level only.

Description

The Restore from Selective Backup option allows you to restore data that was selectively backed up to tape.

Note: If you want to restore your system using the data from a full or partial backup, you must use the Restore from backup utility available on the Install/data tape. For more information on this utility, refer to the *System Installation and Modification Guide* (NTP 555-7001-215).

Change System Administrator Password

Administration level

You can change the system administrator password from the System Administration level only.

Description

The Change System Administrator Password option allows you to change the password for the administration terminal. Your password should be changed on a regular basis to ensure maximum security.

Change Customer Administrator Password

Administration level

You can change the customer administrator password from the System Administration level and Customer Administration level.

Description

The Change Customer Administrator Password option allows you to change the customer password for the administration terminal. Your password should be changed on a regular basis to ensure maximum security.

Change AdminPlus Download Password

Administration level

You can change the AdminPlus password from the System Administration level only.

Description

The Change AdminPlus Download Password option allows you to change the password used by Meridian Mail Reporter (MMR) to download data from the system. The same password must be set up on the MMR side before data can be downloaded. This password must be set up when the system is installed as the default value will not allow the download to take place.

Note: This option only appears if the AdminPlus feature is installed.

Change System Time

Administration level

You can change the system time from the System Administration level only.

Description

The Change System Time option allows you to change your system time.

Dialing Translation

Administration level

Translation tables apply to all customers and can only be configured at the System Administration level.

Description

If Fax on Demand or AMIS Networking, or both, are installed, you must set up translation tables. These tables tell Meridian Mail how to translate collected digits (from an AMIS message header or a fax callback number entered by a caller) into a number that Meridian Mail can dial.

Note: In Meridian Mail 12, this option appears for all Meridian 1 systems.

Related chapters

The following table describes which chapter you should refer to when using one of the General Administration menu options.

For the following option	See
General Options	Chapter 14, “General options.”
Volume and Selective Backup	Chapter 16, “Back up and restore Meridian Mail data.”
Restore from Selective Backup	Chapter 16, “Back up and restore Meridian Mail data.”
Change System Administrator Password	Chapter 17, “Password and system time changes.”
Change Customer Administrator Password	Chapter 17, “Password and system time changes.”
Set Minimum Length for Administrator Passwords	Chapter 17, “Password and system time changes.”

For the following option	See
Change AdminPlus Download Password	Chapter 17, “Password and system time changes.” For more information on Meridian Mail Reporter, refer to the MMR document (P0847870).
Change System Time	Chapter 17, “Password and system time changes.”
Dialing Translation	Chapter 18, “Dialing translations.”

Chapter 14

General options

In this chapter

Overview	14-2
Section A: Setting general options for the system	14-3
Section B: Setting general options for customers	14-21

Overview

Administration level

The General Options screen is available at both the System Administration level and the Customer Administration level. Some general options are applicable to the system as a whole, whereas others must be configured for each customer.

System administration

You can do the following at the System Administration level:

- modify the system name
- define the system addressing length
- choose the ACCESS default customer number
- set the minimum administration password length
- allow/not allow the use of duplicate user DNs
- choose the Integrated Mailbox Administration default customer number
- view a list of installed features
- choose the date format for reports
- define the SEER printer and Reports printer port names

Customer administration

You can do the following at the Customer Administration level:

- modify the customer name
- modify the customer type
- enable the following features (if installed) for each customer:
  - Voice Menus and Announcements
  - Voice Forms
  - Fax on Demand
  - Meridian Mail Networking
- define the attendant DN
- assign up to 15 classes of service to each customer

Modifying general options

Review the default settings in the General Options screen to see which fields you need to modify in order to customize the system to satisfy your requirements.

Section A: Setting general options for the system

In this section

Accessing the General Options screen	14-4
Modifying the system name and system number	14-6
Defining the system addressing length and the supervised transfer delay	14-9
Setting the default customer number for IMA and ACCESS	14-12
Verifying installed features	14-14
Setting the date format for reports	14-16
Setting printer port names	14-18

Accessing the General Options screen

Introduction

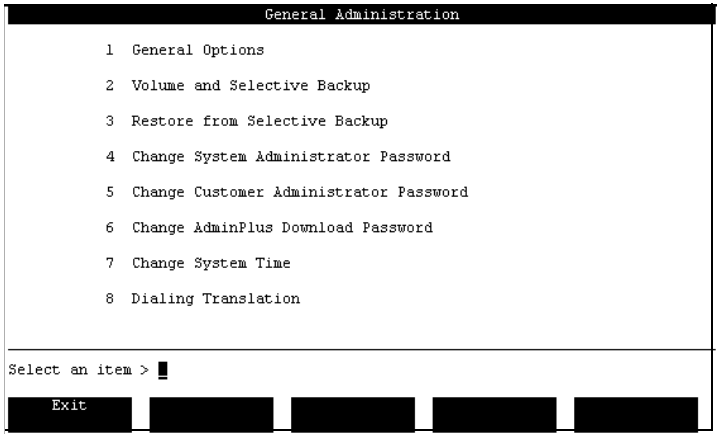
All of the procedures in this section are performed from the General Options screen at the System Administration level.

Procedure

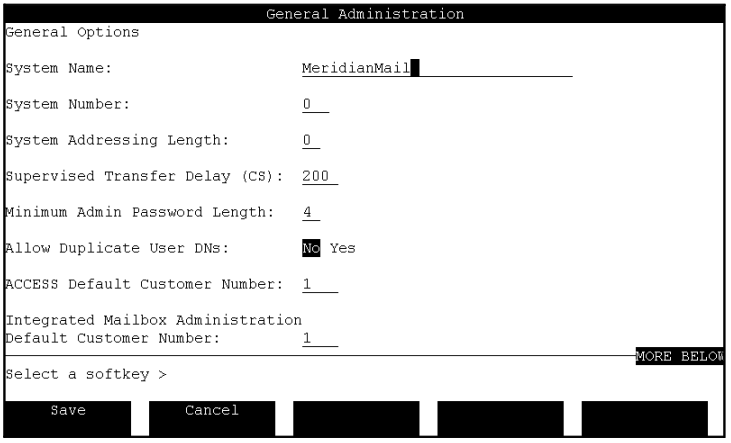
To access the General Options screen at the System Administration level, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration and press <Return>. **Result:** The General Administration menu is displayed.



Step	Action
2	Select General Options and press Return. **Result:** The General Options screen is displayed.



Modifying the system name and system number

Introduction

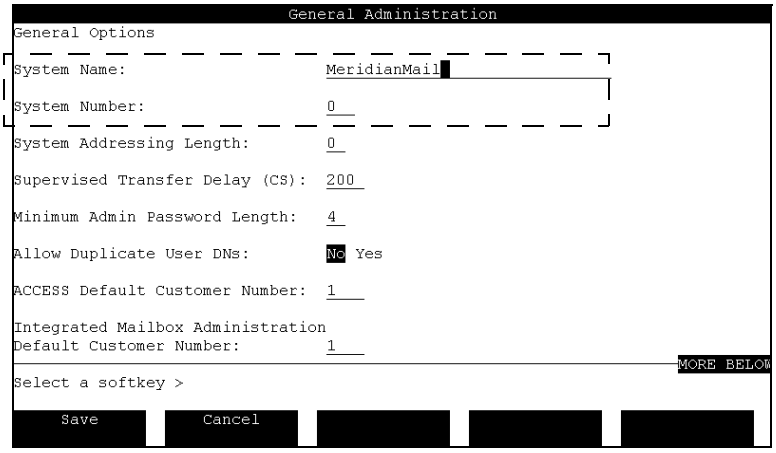
The system name and system number are defined during installation.

When to use

Use this procedure if you need to modify the system name or number, or both, from the values defined during installation.

The General Options screen

The dotted box highlights the fields in the General Options screen that are used to define the system name and number.



Field descriptions

This table describes the fields used to define the system name and number.

System Name	
Description	This is the name by which Meridian Mail is identified. This name is printed on all reports and lists in Meridian Mail.
Default	The name supplied during installation.
Maximum length	You can enter up to 30 alphanumeric characters.

System Number	
Description	This field is prefilled with the number supplied during system installation. The system number must match the Meridian 1's customer number.
Attention	Because this number is entered during installation, you should not have to change it. If there is a mismatch with the Meridian 1's customer number, certain Meridian Mail features that dial out (such as call sender and thru-dial) will not work.
Default	The value supplied during installation.

Procedure

To change the system name or number, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Delete the current name and enter the new name in the System Name field.
2	Change the system number, if necessary. **Attention:** The system number must equal the Meridian 1 customer number. **Note:** If you modify the system number, you must reboot the system for the change to take effect.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Defining the system addressing length and the supervised transfer delay

System addressing length

The system addressing length is intended for Meridian Mail systems connected to DMS-family and SL-100 switches. When set to a non-zero value, the address expansion feature is enabled.

Address expansion is used on systems where the local addressing lengths are shorter than the system addressing lengths.

Meridian 1

For systems connected to Meridian 1 PBXs, the system addressing length should be set to 0 to disable address expansion. This is the default.

Supervised transfer delay

Usage

This transfer delay is used by ACCESS applications when transferring a call to a non-local telset. It is important in cases where the telset to which the call is transferred is busy.

Meridian Mail 11 and 12 versus prior releases

In releases prior to Meridian Mail 11, this delay was set to 200 centi-seconds (2 seconds) and could not be modified.

Default and range

200 centi-seconds is now the default, but it can be modified (to a value between 100 and 1000 centi-seconds, or 1 to 10 seconds).

Centi-seconds

A centi-second is 1/100th of a second. Therefore, 100 centi-seconds equals 1 second.

Do you need to change the default?

If you get reports of callers hearing busy signals when transferred from an ACCESS application to a telset, you need to increase this value.

Finding the right value for your system may take some trial and error. Try incrementing this value by 50 or 100 centi-seconds until you find a setting that works for your system.

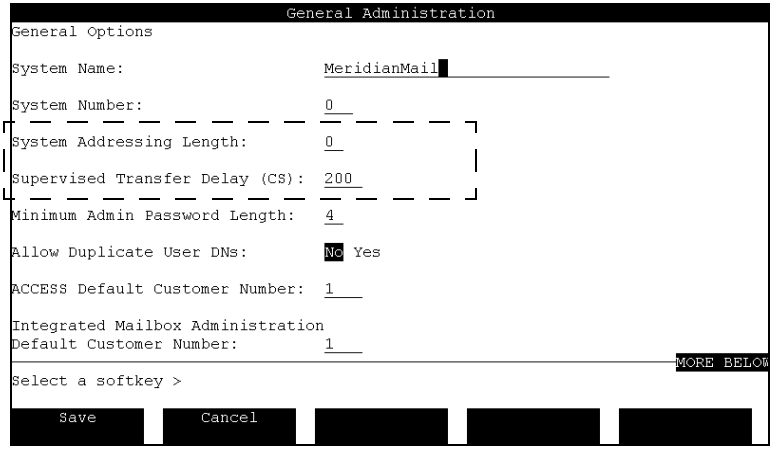
How it works

When an ACCESS application transfers a call off-switch, it waits for the amount of time specified in the delay field. If the telset is busy, a certain amount of time is required to detect the busy signal.

If the delay is not long enough, the busy signal is not detected, the call is transferred to the telset, and the caller hears the busy signal. When the busy signal is detected, the transfer is denied.

The General Options screen

The dotted box highlights the fields in the General Options screen in which you define the system addressing length and supervised transfer delay.



Procedure

To change the system addressing length and supervised transfer delay, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Leave the system addressing length as 0.
2	If the current delay is too short to detect busy signals, then increase the value in the Supervised Transfer Delay field.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

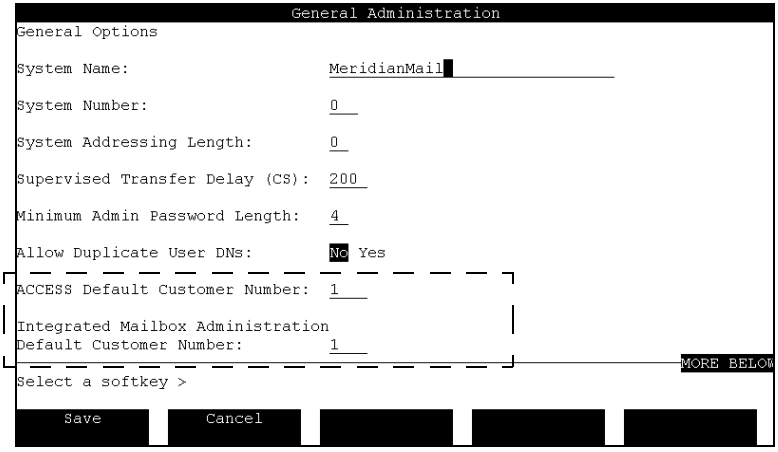
Setting the default customer number for IMA and ACCESS

Introduction

If ACCESS or Integrated Mailbox Administration, or both, are installed, you must specify the default customer number for each.

The General Options screen

The dotted box highlights the field in which the default customer is specified for IMA and ACCESS.



Field descriptions

This table describes the fields in which you enter the default customer numbers for ACCESS and IMA.

ACCESS Default Customer Number	
Description	If an ACCESS application does not specify a customer number, this is the customer to which the application applies.
Default	1
Valid range	1 to 2000

Integrated Mailbox Administration Default Customer Number	
Description	This is the customer to which mailboxes are added when users are added at the M1 terminal using the VMBA feature (in X11). VMBA corresponds to IMA in Meridian Mail.
Default	1
Valid range	1 to 2000

Procedure

To set the default customer number, follow these steps.

Starting Point: General Options screen

Step	Action
1	Enter the number of the customer to which ACCESS applications should apply if no customer number is defined in the application.
2	Enter the number of the customer to which mailboxes should be added when adding users at the M1 terminal using VMBA.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

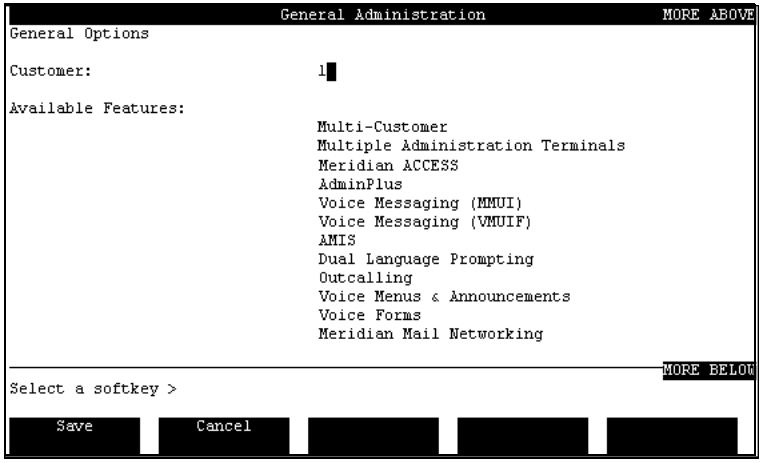
Verifying installed features

When to use

Use this procedure if you need to verify the features that are installed on your system.

The General Options screen

View the list of Available Features in the General Options screen.



Possible features

These are the features that may be installed on your system:

- Multi-Customer
- Multiple Administration Terminals
- Disk To Disk Backup
- Meridian ACCESS (Unix Access)
- AdminPlus
- Meridian Mail AutoAdmin
- Integrated Mailbox Administration
- Voice Messaging (MMUI)
- Voice Messaging (VMUIF)
- Hospitality

  Note: Voice Messaging (MMUI), Voice Messaging (VMUIF), and Hospitality are mutually exclusive and cannot be installed on the same system.

- Voice Menus and Announcements

  This feature allows you to create the following voice services: Voice Menus, Announcements, Thru-Dial services, Time-of-Day Controllers, Prompt Maintenance, and Remote Activation.
- Voice Forms
- Fax on Demand

  This enables a number of fax-related services: Fax Information Service, Fax Item Maintenance Service, Fax Call Back Delivery, and Fax Same Call Delivery.
- Meridian Mail Networking (not available for VMUIF customer groups)

To make the following features available to users, certain fields must be enabled in the user's class of service:

- AMIS
- Dual Language Prompting (MMUI only)
- Outcalling (includes Remote Notification and Delivery to Non-User)

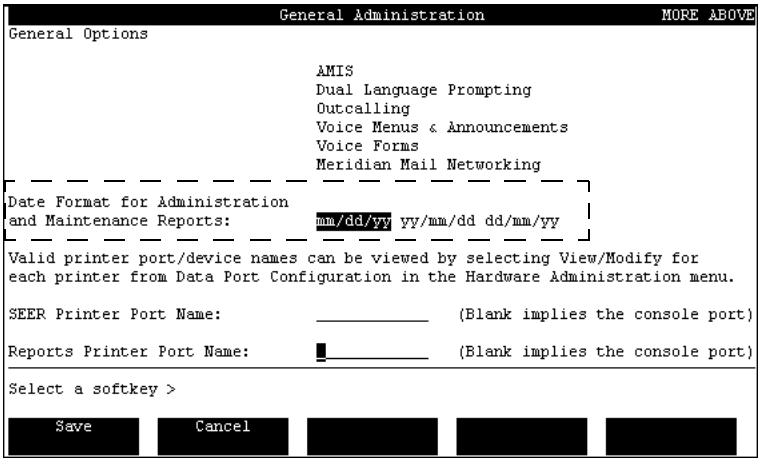
Setting the date format for reports

Introduction

The date format that is selected in General Options is used on administration and maintenance reports.

The General Options screen

The dotted box highlights the field in which you specify the date format.



Field description

The format selected in the Date Format for Administration and Maintenance Reports field affects the following:

- reports generated by Meridian Mail (including operational measurements)
- SEERs
- the format for inputting dates in Meridian Mail screens

Default

The default is mm/dd/yy.

Valid options

You can choose from the following date formats:

- mm/dd/yy (default)
- yy/mm/dd
- dd/mm/yy

Procedure

To change the date format, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the date format field.
2	Select the date format you want used on reports and in screens.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Setting printer port names

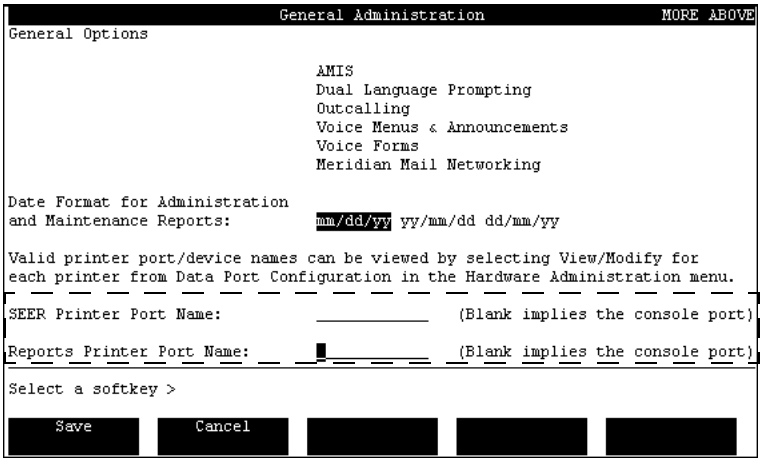
Introduction

You can define separate printer port names for a SEER printer and a reports printer.

If you do not define these printer port names, SEERs and reports are printed to the console printer port.

The General Options screen

The dotted box highlights the fields in which printer port names are defined.



Field descriptions

This table describes the printer port name fields.

SEER Printer Port Name	
Description	This is the printer port to which the SEER printer is connected.
Requirement	You must have additional data ports on an RSM card to support a SEER printer. They must be defined as printer ports in the hardware database.
Default	Blank If this field is left blank, the SEERs will print to the console printer port.
Maximum length	The printer port name may be up to 12 alphanumeric characters long.

Reports Printer Port Name	
Description	This is the printer port to which the Reports printer is connected. Operational measurements and general print jobs are sent to this printer.
Requirement	Additional data ports on an RSM card are required. The data ports must be defined as printer ports in the hardware database.
Default	Blank If this field is left blank, the reports will print to the console printer port.
Maximum length	You can enter a printer port name up to 12 alphanumeric characters long.

Procedure

To set or change the printer port names, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the printer name field to be modified.
2	Have you set up a special printer for SEERs? • If yes, enter its port name in the SEER Printer Port Name field. • If no, leave this field blank and proceed to the next step.
3	Have you set up a special printer for printing reports? • If yes, enter its port name in the Reports Printer Port Name field. • If no, leave this field blank and proceed to the next step.
4	You are finished defining general options for the system. Do you want to save your changes? • If yes, press [Save] to save your changes and return to the General Administration menu. Go to the next section to modify general options for customers. • If no, press [Cancel] to return to the General Administration menu without saving your changes.

Section B: Setting general options for customers

In this section

Overview	14-22
Accessing the General Options screen at the customer administration level	14-23
Modifying the customer name and customer type	14-25
Enabling and disabling optional features for customers	14-27
Assigning classes of service to customers	14-29
Setting the attendant DN	14-31

Overview

Introduction

Fields that are configured in the General Options screen at the System Administration level are displayed in the General Options screen at the Customer Administration level, but are read-only and cannot be modified.

Read-only fields

The following fields are read-only:

- System Name
- System Number
- System Addressing Length
- Supervised Transfer Delay
- Minimum Admin Password Length
- Allow Duplicate User DNs
- ACCESS Default Customer Number
- Integrated Mailbox Administration Default Customer Number
- Customer Number
- Interface Type
- Date Format for Administration and Maintenance Reports
- SEER Printer Port Name
- Reports Printer Port Name

Customer-level general options

You can do the following for each customer in the General Options screen at the Customer Administration level:

- modify the customer name and type
- enable optional features
- assign classes of service to customers
- set the attendant DN

Accessing the General Options screen at the customer administration level

When to use

The procedures in this section are carried out for each customer.

Use this procedure to access the General Options screen at the Customer Administration level.

Before you begin

You must first select the customer you want to modify.

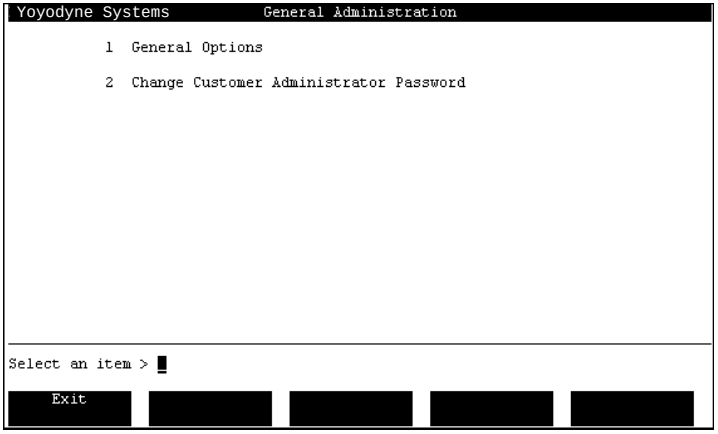
See “Selecting a customer to view or modify” on page 5-17.

Procedure

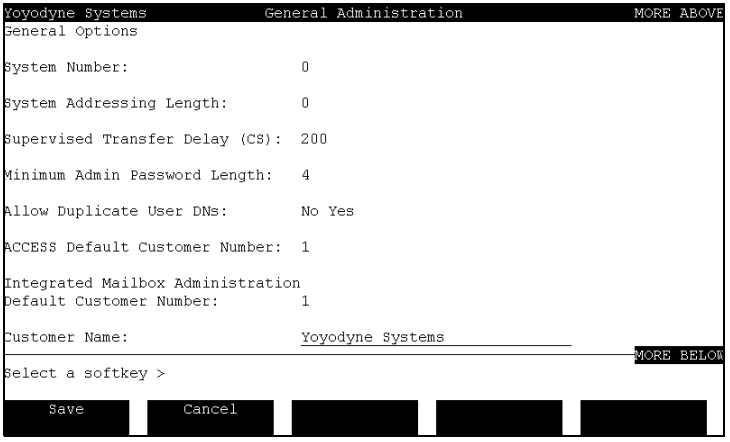
To access the General Options screen, follow these steps.

Starting Point: The Customer Administration Menu

Step	Action
1	Select General Administration and press <Return>. **Result:** The General Administration menu appears.



2	Select General Options and press <Return>. **Result:** The General Options screen appears.



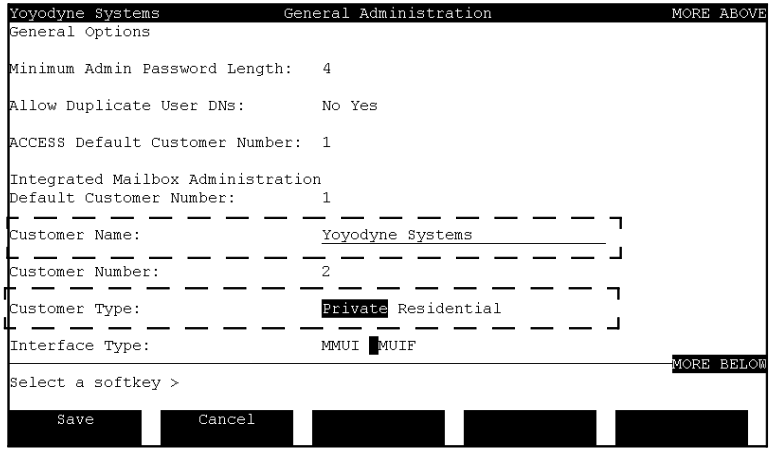
Modifying the customer name and customer type

When to use

The customer name and customer type are defined when you add a customer. Once the customer has been defined, you can change the name and type using this procedure.

The General Options screen

The dotted box highlights the fields in which you change the customer name and type.



Field descriptions

This table describes the fields in which you change the customer number and type.

Customer Name	
Description	The name of the customer.
Default	The name entered when the customer was added.
Maximum length	30 characters

Customer Type	
Description	The type of customer.
Default	The type selected when the customer was added.
Valid options	Private, Residential, Hospitality (if installed) • ***Private*** is intended for centrex customers. • ***Residential*** is intended for residential customers. When this option is selected, users do not have access to name dialing or name addressing, even if the interface type is MMUI. • ***Hospitality*** is intended for the hospitality (hotel) industry. This option can only be selected for one customer, since Hospitality can only be enabled for one customer.

Procedure

To modify the customer name, number, or type, follow these steps.

Starting Point: General Options screen

Step	Action
1	Delete the current customer name and enter the new name in the Customer Name field.
2	Change the customer type if necessary.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Enabling and disabling optional features for customers

Introduction

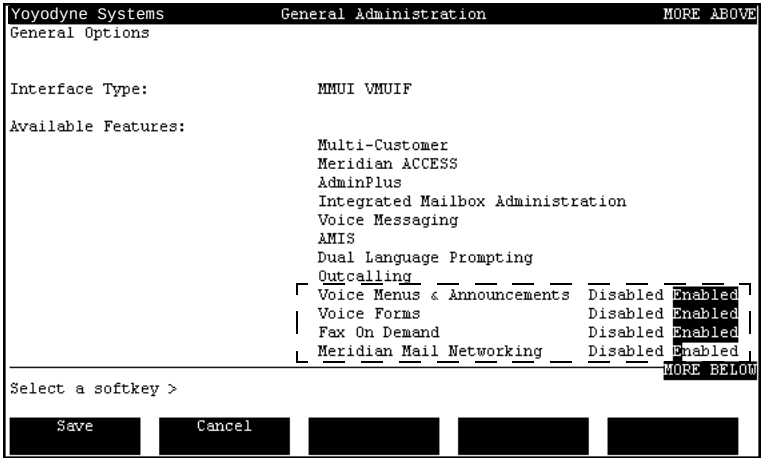
The following features (if installed on the system) are enabled and disabled on a customer-by-customer basis:

- Voice menus and announcements
- Fax on Demand
- Voice Forms
- Meridian Mail Networking

All other installed features are enabled for all customers.

The General Options screen

The dotted box highlights the fields in which you enable optional features for customers.



Defaults

These optional features are disabled for all customers by default.

Procedure

To enable optional features for customers, follow these steps.

Starting Point: General Options screen

Step	Action
1	Move the cursor to the feature (in the Available Features) list that you want to enable or disable.
2	If you want to enable a feature, use the left and right arrow keys to select Enabled.
3	If you want to disable a feature, use the left and right arrow keys to select Disabled.
4	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Assigning classes of service to customers

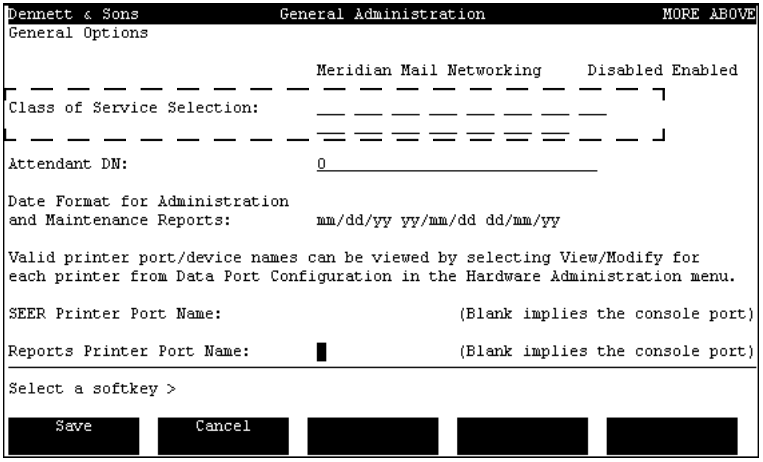
Introduction

Once you have created Meridian Mail classes of service (through Class of Service Administration), you must assign them to each customer. Otherwise, they will not be available when you add local voice users.

You can add up to 15 classes of service to each customer.

The General Options screen

The dotted box highlights the fields in which you assign classes of service to customers.



Field description

You enter the classes of service that you want to assign to the customer in the Class of Service Selection fields.

When adding local voice users, you will assign them to one of the COSs specified here.

Default

All fields are blank.

Maximum number of classes of service

You can enter up to 15 classes of service in these fields.

Procedure

To assign classes of service, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the Class of Service Selection field.
2	Enter up to 15 classes of service in the Class of Service Selection fields.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Setting the attendant DN

The attendant DN

The Attendant DN is the extension number to which a caller is transferred when the user's revert DN is unsuccessful or undefined.

The revert DN

When adding users, you can define a unique revert DN for each user. If the Custom Revert DN feature is enabled, users can define their own revert DNs from their telsets.

When the attendant DN is used

The Attendant DN that is defined in General Options is used if the revert DN is not defined or the call is not successfully transferred to the user's revert DN.

The revert DN and attendant DN are used under two conditions.

Call answering

A caller can press "0" during a call answering session in order to transfer to another number (such as that of an attendant or secretary). This gives callers the chance to transfer to a person for assistance.

Mailbox thru-dial (extension dialing)

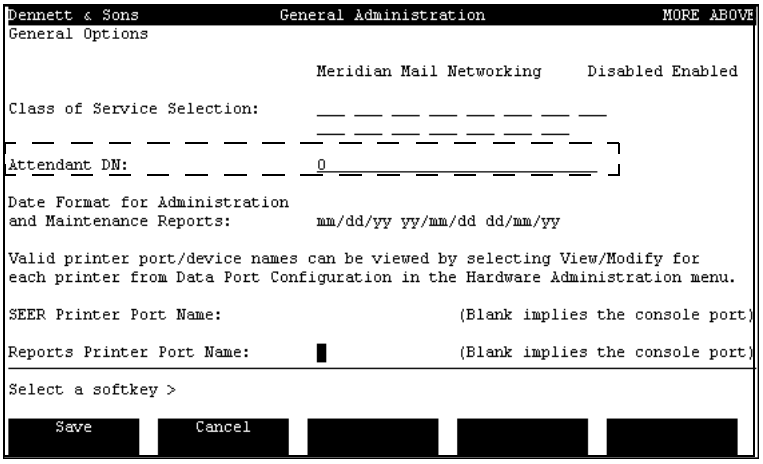
Mailbox thru-dial allows MMUI users to dial a number while they are logged into their mailbox. The user enters "0" followed by the number. If the user waits for more than 2 seconds after entering "0", he or she is transferred to the revert DN.

See also

For more information, see "The revert DN" on page 9-23.

The General Options screen

The dotted box highlights the field in which you define the Attendant DN.


Dennett & Sons General Administration MORE ABOVE
General Options
Meridian Mail Networking Disabled Enabled
Class of Service Selection:
Attendant DN: 0
Date Format for Administration
and Maintenance Reports: mm/dd/yy yy/mm/dd dd/mm/yy
Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.
SEER Printer Port Name: (Blank implies the console port)
Reports Printer Port Name: (Blank implies the console port)
Select a softkey >
Save
Cancel

Field description

This field may be left blank. However, it is recommended that you define this DN so that it can serve as a backup if the user's revert DN is not defined or unsuccessful.

Maximum length

You can enter a DN that is up to 30 digits in length. This DN can begin with 0.

Default

0

Procedure

To change the attendant DN, follow these steps.

Starting Point: General Options screen

Step	Action
1	Use the cursor keys to move to the Attendant DN field.
2	Do you want to revert callers to a DN other than 0? • If yes, delete the current DN and enter the new DN in the Attendant DN field. • If no, leave the Attendant DN field set to 0.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Chapter 15

Volume administration

In this chapter

Overview	15-2
Volume names	15-3
Volume contents	15-5
Volume distribution on single- and multi-node systems	15-7
Voice storage capacity in single- and multi-node systems	15-8
Checking volume capacity and usage levels for your system	15-10

Overview

Introduction

Meridian Mail systems can have from one to five nodes, each of which contains a hard disk drive for data storage. The hard disk drives are partitioned into volumes. Volumes are storage areas for system and user-related information.

Volume administration involves making backup copies of some or all of the data stored on a hard disk. If a disk fails, data can be restored from the backup so that the system can be brought back into service quickly with minimal loss of information.

Administration level

You can access Volume Administration from the System Administration level only.

Volume names

Introduction

Volume names are used to identify volume partitions on hard disk drives. The volumes are already set up when your Meridian Mail system is installed.

Definition

Each hard disk on each node is partitioned into two volume types: system and user. Volume names follow specific formats to ensure easy identification when backing up the system.

In the first node, the system volume is named VS1 and the user volume is named VS2.

In three-node, four-node, and five-node configurations, the disk drive on the first node contains no user volume. Volumes on nodes other than the first node are named VStnnX.

Components

Volume names consist of four components. These four components are listed in the following table.

Component	Description
VS	Volume server
t	The first digit in the volume name indicates the type of information stored on the volume. Possible digits are 1 system information 2 user information 9 disk-to-disk backup (if installed, for partial backup)
nn	The last two digits in the volume number indicate the node number.
X	The region on the volume, either T for text data, or V for voice data.

Example

VS205T refers to the text region (T) of a user volume (2) on node 5 (05).

Name exceptions

There are some special cases where volume names differ from the standard volume name format.

These are the exceptions:

- User volume on node 1 is labeled VS2.
- System volume on node 1 is labeled VS1.
- Full backup of VS1 creates volume backup labels B102V and B102T.

Volume contents

Introduction

The two types of volumes, system and user, contain different sets of information. For backup purposes, it is important to be aware of the type of information stored on each volume type.

System volume

The system volume VS1 contains the user information listed below:

- each user's personal verification
- system profile
- customer profiles
- corporate directory
- operation measurement traffic and billing data
- program software
- network database*
- voice menus and announcements*
- voice forms*
- fax items*
- network message queues
- voice prompts for third and fourth languages*

Items marked with an asterisk (*) may not be installed and stored on VS1, depending on how your system was set up.

Note: Voice services (voice menus, voice forms, fax items) are stored on VS1 by default. However, they can be moved to another volume if there is not enough space on VS1.

User volumes

The user volumes (VS2, VS202, VS203, VS204, VS205) can contain the following information:

- messages
- greetings
- voice services (voice menus, voice forms, fax items) which may be moved from VS1 to VS2 or VS202 if voice services require more space than is available on VS1
- user information
- voice prompts for first and second languages (on VS2 only)
- voice form responses

Volume distribution on single- and multi-node systems

Introduction Single-node and multi-node systems contain different volume configurations.

Node contents The following table shows the possible volume configuration for each node.

System	Node 1	Node 2	Node 3	Node 4	Node 5
Single-node	VS1 - system VS2 - user				
Two-node	VS1 - system VS2 - user VS901- backup	VS202 - user VS902 - backup			
Three-node	VS1 - system VS2 - system VS901 - backup	VS202 - user	VS203 - user		
Four-node	VS1 - system VS2 - system VS901 - backup	VS202 - user	VS203 - user	VS204 - user	
Five-node	VS1 - system VS2 - system VS901- backup	VS202 - user	VS203 - user	VS204 - user	VS205 - user

Voice storage capacity in single- and multi-node systems

Voice storage capacity The following table shows the voice storage capacity for single-node and multi-node systems.

Voice Storage capacity		Maximum hours available for voice storage (per disk volume)						
System Size	**Total hours per volume**	**VS1**	**VS2**	**VS202**		**VS203**	**VS204**	**VS205**
1-node 1.2 Gbyte disk (EC and ModOp)	5 11 24 36 54 100 200*	2 2 3.5 3.5 3.5 5.5 10.2	5 11 24 36 54 100 200					
2-node 1.2 Gbyte disk (EC and ModOp)	26 54 84 114 200 400*	2 3.5 3.5 3.5 5.5 10.2	11 24 24 54 100 200	15 30 60 60 100 200	n/a 22.2 52.2 52.2 90.1 184.8			
3-node 1.2 Gbyte disk (EC and ModOp)	30 60 90 120 200 400*	18.4 18.4 18.4 18.4 18.4 51.9		15 30 60 60 100 200	n/a 6.3 36.3 36.3 76.3 142.4	15 30 30 60 100 200		
4-node 1.2 Gbyte disk (EC and ModOp)	45 90 120 180 300 600*	18.4 18.4 18.4 18.4 18.4 68.6		15 30 60 60 100 200	n/a 5.3 35.3 35.3 75.3 124.5	15 30 30 60 100 200	15 30 30 60 100 200	

Voice Storage capacity		Maximum hours available for voice storage (per disk volume)						
System Size	**Total hours per volume**	**VS1**	**VS2**	**VS202**		**VS203**	**VS204**	**VS205**
5-node 1.2 Gbyte disk (EC and ModOp)	60 120 180 240 400 800*	19.6 19.6 19.6 19.6 19.6 86.6		15 30 60 60 100 200	— 2.4 32.4 32.4 72.4 104.6	15 30 30 60 100 200	15 30 30 60 100 200	15 30 60 60 100 200
Note: VS202 lists two columns of figures. The first column is without disk-to-disk backup. The second column is with disk-to-disk backup.								
* — A 2.0 Gbyte disk is required for each of these configurations.								

Additional language exceptions

The number of languages your system uses has an impact on the available volume capacity for each hard disk.

If your system has three or more nodes and a second language installed, subtract three hours from the volume capacity of VS2. If your system only has one or two nodes, then subtract three hours from the volume capacity of VS1.

If your system has a third language installed, subtract three hours from VS1, and an additional three hours for the fourth language.

Checking volume capacity and usage levels for your system

Description

The Volume and Selective Backup screen displays all the volumes on your system, their designated use, their capacity in kbytes and equivalent hours and minutes, and the percentage of voice and data storage currently used.

Administration level

You can access the Volume and Selective Backup screen from the System Administration level only.

Accessing the Volume and Selective Backup screen

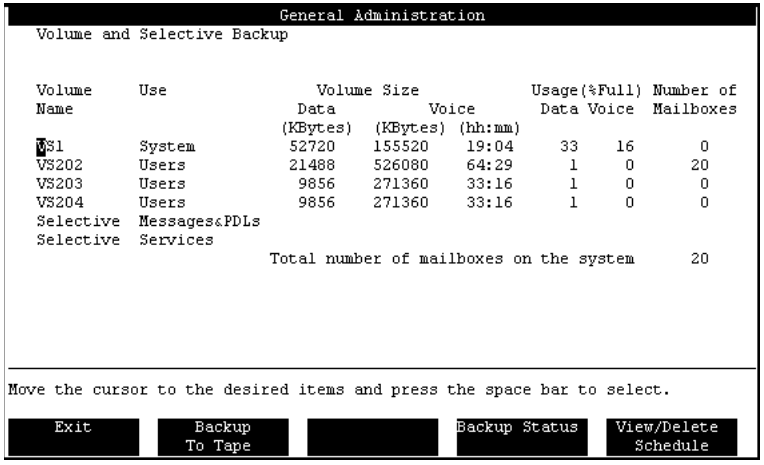
To access the Volume and Selective Backup screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen is displayed.

Volume and Selective Backup screen

The following shows the Volume and Selective Backup screen.



Field descriptions

This table describes the fields in the Volume and Selective Backup screen.

Volume Name	
Description	Displays the name of the volume. The volume name indicates the type of data contained on the volume, and the node on which it resides.
Format	Volume names are in the format VSTnn. The region of the volume (x) is not displayed.
Valid options	Any of the listed volumes.

Use	
Description	Describes the type of volume, either system or user.

Volume Size Data (kbytes)	
Description	Displays the amount of storage allocated for blocks of data on the volume.
Measurement	Storage is expressed in thousands of bytes (kbytes).

Volume Size Voice (kbytes)	
Description	Displays the amount of storage allocated for blocks of voice data on the volume.
Measurement	Storage is expressed in thousands of bytes (kbytes).

Volume Size Voice (hh:mm)	
Description	Displays the amount of storage allocated for blocks of voice data on the volume.
Measurement	Storage is expressed in hours and minutes.

Usage (% Full) Data	
Description	Displays the percentage of allocated data storage currently in use.

Usage (% Full) Voice	
Description	Displays the percentage of allocated voice storage currently in use.

Number of Mailboxes	
Description	Displays the number of local voice users on the volume.
Dependency	This number is dependent on the number of voice users configured for your system.

Total number of mailboxes on the system	
Description	Displays the total number of mailboxes on the system.

Checking disk capacity and usage levels

For information on checking disk capacity and usage levels for your system, see “Disk Usage Detail report” on page 32-52.

Chapter 16

Back up and restore Meridian Mail data

In this chapter

Overview	16-2
Section A: Preparing for backups	16-3
Section B: Full and partial backups to tape	16-15
Section C: Selective backup of users and services	16-23
Section D: Partial backups to disk	16-39
Section E: Scheduled backups	16-41
Section F: Backup maintenance	16-47
Section G: Restoring information from a Selective backup	16-53

Overview

Description

This chapter

- explains the importance of Meridian Mail system backups
- suggests which volumes to back up, and how frequently
- describes selective backup of mailboxes and services
- describes the two available backup media, and how to perform a backup with either one
- describes the procedures for scheduling a backup to occur automatically at a later time, and for checking on the status of a backup in progress
- describes procedures for restoring selective backup data from backup media (disk or tape) back to the Meridian Mail system

Section A: Preparing for backups

In this section

Overview	16-4
The three types of backups	16-5
Selective backup	16-6
Partial backup	16-8
Full backup	16-9
Volumes to back up	16-10
How often to do backups	16-11
Disk backup or tape backup	16-13
Before you perform a backup	16-14

Overview

Introduction

This section describes the three types of backups: selective, partial, and full.

It is important to perform backups regularly as they provide a safeguard against disk failure. Recovery from a system where no backups have been made entails a complete reentry of all user and site-specific information.

Administration level

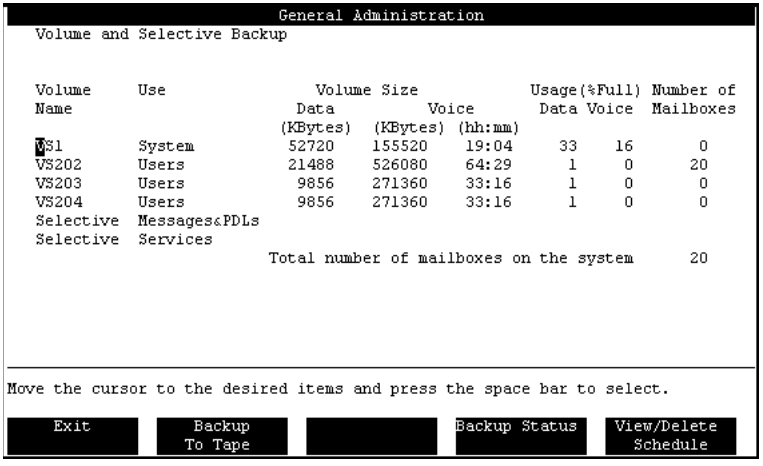
You can perform backups from the System Administration level only.

Nightly audits

Nightly VS audits have been modified to permit an overnight full backup. If a backup is running, the VS audit will be repeatedly delayed until either the backup completes or a specified time limit, set upon installation, is reached, (around 4:30 a.m.). If the time limit is reached, the VS audit will force the backup to be aborted. Previously, overnight full backups were likely to fail due to a conflict with one of the automatic nightly VS audits.

The Volume and Selective Backup screen

The following is an example of the Volume and Selective Backup screen where backup options are accessed.



The three types of backups

Introduction

There are three types of backups that can be performed:

- selective
- partial
- full

Description

The three backup options allow you to select the appropriate type for your backup without always having to perform a full backup.

Selective backup

Selective backups allow you to back up user messages, personal distribution lists, and multimedia services. Selective backup also enables you to back up mailboxes by specific criteria (such as volume or department).

Partial backup

Partial backups save the administration configuration of the system, including the system volume and user profiles. This type of backup saves user data only, not voice.

Full backup

Full backups back up all volumes on your system, including voice and data from system and user volumes.

Selective backup

Introduction

The selective backup option provides online backups for user messages, personal distribution lists (PDLs), and multimedia services.

Description

The selective backup feature provides you with considerable flexibility in backing up data. User messages, PDLs, and multimedia services may be backed up at any time or as part of the regular backup schedule.

Backup criteria for messages and PDLs

To use the selective backup option, you must select a criteria by which to back up from the list below. You can select only one criteria per selective backup, and this criteria defines the content to be backed up:

- all messages and PDLs of all users on the system
- by volume, up to the total number of volumes on the system
- by classes of service, up to 15
- by departments, up to five input areas. The wildcards '+' and '_' are permitted so that more than five departments may be backed up.
- by individually specified mailboxes, up to 10 input areas. The wildcards '+' and '_' are permitted so that more than 10 mailboxes may be backed up.

Note: Only one wildcard can be used per input field, and it should be the last character.

Example

Valid	Invalid
805+	80+1
805_	80_1

Backup criteria for voice services

One of the following criteria must be selected for the selective backup of voice services:

- all voice services on the system
- by service ID, up to 30 input areas. The wildcards '+' and '_' are permitted so that more than 30 services may be backed up.

Note: Only one wildcard can be used per input field, and it should be the last character.

Example

Valid	Invalid
805+	80+1
805_	80_1

Backup order

If a selective backup is chosen together with a regular backup, the volume backups will always be done first. The selective backup will always be the last backup on the tape.

Partial backup

Introduction

Partial backups allow you to back up and save the administration configuration of your system. It will back up the system volume and user profiles. During a restore, this avoids having to reenter user information; however, all voice messages and user greetings will be lost.

Data that is backed up

When you perform a partial backup, you save the administration configuration of the system including the following:

- the user database
- spoken names (personal verification)
- voice services (voice menus, voice forms, fax items) if stored on VS1

Volumes that are backed up

A partial backup saves the following volumes:

- VS1T
- VS1V
- VS1B
- VS901T

Exceptions

Partial backups do not back up the following information:

- users' voice data (including voice messages and greetings)
- voice services (voice menus, voice forms, fax items) if stored on a volume other than VS1

Full backup

Introduction

A full backup is used to back up all system and user voice and data on the entire system. A full backup is not normally done unless significant changes have been made to your system.

Data that is backed up

A full backup backs up all system data including

- the user database
- spoken names (personal verification)
- voice services (voice menus, voice forms, fax items)
- users' voice data (including voice messages and greetings)

Volumes that are backed up

A full backup saves the following volumes:

- VS1T
- VS1V
- VS1B
- all VSxT, VSxV, and VSxB, where x is 2 or 202 through 205, depending on the number of nodes in your system.

VS1B

VS1B is a temporary volume that is created during backup and is copied to tape. It is automatically deleted from disk once the backup is complete.

Exceptions

Normally, full backups are not done because user messages and greetings are transitory and do not warrant the extra time required to back them up.

CAUTION

Risk of data loss

If the loss of messages carries financial or legal implications, weekly or even daily backups of voice data may be warrranted.

Volumes to back up

Introduction

Backups are essential to safeguard your system against disk failure. It is important to back up volumes with all necessary system and user voice and data information.

Volumes recommended for regular backup

The following table shows the recommended volumes for backup on single-node, two-node, three-node, four-node, and five-node systems.

Volumes marked with * store data unless voice services are installed there, in which case you select Voice and Data, rather than Data.

Single-node system	Two-node system	Three-node system	Four-node system	Five-node system
VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data
VS2 - Data *	VS2 - Data *	VS202 - Data *	VS202 - Data *	VS202 - Data
	VS202 - Data *	VS203 - Data *	VS203 - Data *	VS203 - Data *
			VS204 - Data *	VS204 - Data *
				VS205 - Data *

How often to do backups

Introduction

Backups should be performed regularly. Recovery from a system where no backups have been made entails a complete reentry of all user and site-specific information.

Nightly audits

Nightly VS audits have been modified to permit an overnight full backup. If a backup is running, the VS audit will be repeatedly delayed until either the backup completes, or a specified time limit, set upon installation, is reached (around 4:30 a.m.). If the time limit is reached, the VS audit will force the backup to be aborted.

Backup considerations

Keep the following in mind when determining how often and when to do backups:

- Backups should be carried out at a time when the system is relatively quiet, or outside the regular business hours for your organization.
- Do not back up the system while it is being actively used (more than half the ports or channels are active). The system may not have enough resources to complete the backup.
- Backups to disk can be done frequently with relatively little effort, and reduce the need for frequent and time-consuming backups to tape. However, disk-to-disk backups do not eliminate the need for tape backups.

Location of voice services

Verify where voice services (such as voice menus, thru-dialers, and voice forms) are stored.

ATTENTION

If voice services are stored on a volume other than VS1, be sure to do a full backup of that volume, selecting the Voice and Data option.

Administration level

You can verify the location of voice services from the System Administration level only.

Verifying the location of voice services

To verify where voice services are stored, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Select Voice Services Profile.
4	Check the Voice Services Volume field. This is where voice services are stored.

System backup requirements

A field support representative can restore a system to the state it was in at the time of the last backup. To ensure that this recovery process is complete, you should make certain that you have on hand a complete set of backup tapes.

If no backups have been kept, a complete reentry of all user and site-specific information will be required. How often you back up your data is influenced by how often changes are made to user and system information. If you make important changes to the system daily, then daily backups may be in order.

Disk backup or tape backup

Introduction

Meridian Mail offers two types of backups, disk and tape.

Disk backup

Backup to disk can be either partial or selective. To use the backup-to-disk feature, the disk-to-disk option must be installed. Full backups cannot be done to disk and must be backed up using tape.

On multi-node systems, the backup-to-disk option copies selected information from the first hard disk to the second hard disk on the system. This allows for data to be copied from one disk to another in order to allow for recovery after a single disk failure. Backup to disk can be done frequently with relatively little effort, and reduces the need for frequent and time-consuming backups to tape.

Backups to disk do not completely eliminate the need for tape backups.

> **CAUTION**
>
> **Risk of data loss**
>
> If a disk failure occurs in the middle of a disk-to-disk backup, the copy will not be consistent and recovery from this backup copy will not be possible. For this reason, disk-to-tape backups should also be performed periodically.

Tape backup

Backup to tape allows for the backup of the entire Meridian Mail system including voice and data on all volumes. This provides you with a full backup copy of all information needed to restore your system to full working order in case of failure.

All Meridian Mail systems have a tape drive capable of reading and writing industry-standard 1/4-inch data cartridges.

Before you perform a backup

Overview

There are many considerations that need to be taken into account before performing a backup.

Timing

Avoid backing up the system between the hours of 1:00 a.m. and 5:00 a.m. since important system audits take place during these hours.

Do not back up the system when it is operating above 50% of the rated capacity for call answering, voice messaging, and port usage. Try to choose the lowest traffic time outside of the audit hours.

Storage

Backup tapes should be stored in a secure area free of electromagnetic fields. Important backups should be stored off-site for added security.

Store tapes in their cases, label them clearly, and set the write protection tab (turn the rotating knob until the arrow points to Safe).

Other backup considerations

Consider the following before backing up:

- Restoring from a full or partial backup from tape involves downtime as the system is booted from tape and data is restored onto disks one at a time.
- Do not schedule a backup to tape that requires multiple tapes unless you will be around during the backup to switch tapes.
- Do not use Nortel software distribution tapes for backing up your system; these tapes are important for recovering from disk failures.
- Do not reuse the same tapes for consecutive backups. It is recommended that you maintain at least two sets of backup tapes and that you use these sets in rotation.

Section B: Full and partial backups to tape

In this section

Overview	16-16
Performing a full backup to tape	16-18
Performing a partial backup to tape	16-20

Overview

Introduction

This section details information on full and partial backups to tape.

Types of tape drives

Meridian Mail supports two tape drives: the Tandberg TDC4220 drive, and the Archive Viper drive.

The Tandberg TDC4220 drive reads and writes tapes with a capacity up to 2.5 Gbytes and is backwards compatible with all existing Meridian Mail tapes.

The Archive Viper drive supports a maximum storage capacity of 250 Mbytes, and should be used only with DC6250 tapes.

CAUTION

Risk of tape load failure

Use of 6150 tapes may cause tape load failures. 6150 tapes are no longer supported.

Using the Archive Viper tape drive

When using a Viper tape drive, insert the tape with the metal side facing the left side of the drive and the opening on the tape facing up. Once the tape is inserted, secure it by pressing down on the lever on top of the opening until the latch catches. To remove a tape, slide the latch up and the tape will be ejected.

Using the Tandberg tape drive

When using a Tandberg tape drive, press the Release button to open the door. (If there is a tape in the drive already, remove it.) Gently push the tape into the drive and close the door. To remove a tape, press the Release button to open the door and remove the tape.

Write-protection

Tape cartridges can be write-protected by turning the rotating knob on the cartridge until the arrow points to the Safe indicator. Any attempt to write on a write-protected cartridge will generate an error.

Tape errors

If a tape error occurs during backup, you do not have to restart the backup process from tape 1. Follow the instructions as they appear on your screen. In some instances, you are required to keep the tape, as the data that was recorded is not corrupt; in other instances, you will be required to discard the tape. At this stage, you should clean the tape heads before inserting another tape. See “Cleaning/maintaining the tape drive” on page 16-52.

Performing a full backup to tape

Introduction

A full backup to tape backs up all of your system and user voice and data.

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Backup tape requirements and time estimates

The following table lists the backup tape requirements for a full backup for each system.

One full backup (250 Mbyte tapes)					
System	**# Tapes**	**System**	**# Tapes**	**System**	**# Tapes**
1 node		2 node		3 node	
5 h	1	26 h	2	30 h	2
11 h	1	54 h	3	60 h	4
24h	2	84 h	4	90 h	5
36 h	2	114 h	5	120 h	6
54 h	3	200 h	8	200 h	9
100 h	5				
4 node		5 node			
45 h	3	60 h	3		
90 h	5	120 h	5		
120 h	6	180 h	8		
180 h	8	240 h	10		
300 h	12	400 h	16		

Administration level

You can perform a full backup to tape at the System Administration level only.

Procedure

To perform a full backup to tape, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the cursor on the volume you want to back up, and press <Space Bar> to select it. **Note:** It is recommended that you back up only one volume at a time. However, you can select more than one volume.
4	Press [Backup to Tape]. **Result:** The Disk to Tape Backup screen appears.
5	Enter an appropriate label for this backup.
6	Use the arrow keys to move to the Backup Options column. Select Voice and Data for a full backup.
7	Do you want to back up now? • If yes, then press [Immediate Backup] and go to step 8. **Result:** If you select Immediate Backup, the softkeys change to [OK to Start Backup] and [Cancel]. The system also displays how much data (in Mbytes) will be backed up. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for how to insert tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup] to initiate the backup. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape backup screen.
10	When the tape is full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.
11	Repeat this procedure until all volumes have been backed up.

Performing a partial backup to tape

Introduction

A partial backup to tape backs up your system configuration and user information. This backup backs up only user data, and not voice.

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Backup tape requirements and time estimates

The following table lists the backup tape requirement estimates for a partial backup for each system.

One partial backup (250 Mbyte tapes)					
System	# Tapes	System	# Tapes	System	# Tapes
1 node		**2 node**		**3 node**	
5 h	1	26 h	1	30 h	1
11 h	1	54 h	1	60 h	1
24h	1	84 h	1	90 h	1
36 h	1	114 h	1	120 h	1
54 h	1	200 h	1	200 h	1
100 h	1				
4 node		**5 node**			
45 h	1	60 h	1		
90 h	1	120 h	1		
120 h	1	180 h	1		
180 h	1	240 h	1		
300 h	1	400 h	2		

Administration level

You can perform a partial backup to tape at the System Administration level only.

Procedure

To perform a partial backup to tape, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume Administration and Selective Backup. **Result:** The Volume Administration and Selective Backup screen appears.
3	Position the cursor on the volumes you want to back up, and press <Space bar> to select them.
4	Press [Backup to Tape]. **Result:** The Disk to Tape Backup screen appears.
5	Enter an appropriate label for this backup.
6	Use the arrow keys to move to the Backup Options column.
7	Are you backing up the system volume? • If yes, select Voice and Data. • If no (you are backing up a user volume), select Data.
8	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The [OK to Start Backup] and [Cancel] softkeys are displayed. • If no, go to “Scheduling the backup for a later time” on page 16-42.
9	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for how to insert tapes.
10	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
11	When the tape is full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Section C: Selective backup of users and services

In this section

Overview	16-24
Backing up all users	16-25
Backing up individual users	16-27
Backing up all users in a specified volume	16-29
Backing up all users assigned to a particular class of service	16-31
Backing up all users in a specific department	16-33
Backing up all multimedia services	16-35
Backing up selected individual multimedia services	16-37

Overview

Introduction

The selective backup feature allows for the selective backup of user messages, personal distribution lists (PDLs), and multimedia services. Selective backups can be performed as immediate backups or scheduled on a regular basis.

Example

The Selective Backup and Restore feature allows users to request a backup of their messages and PDLs for safekeeping, and can have them restored at any time. If scheduled daily selective backups are being done, the user can request the restore of an accidentally deleted message or PDL and have it restored from the previous day's backup.

Flexibility

The selective backup feature offers new flexibility in backing up and restoring data. User messages, PDLs, and multimedia services may be backed up at any time or as part of the regular backup schedule.

Selective backup criteria

When specifying which data to back up, there are a number of criteria from which to choose. To back up messages and PDLs, one (and only one) of the following criteria may be used:

- all the messages and PDLs of all users on the system
- by volume, up to the total number of volumes on the system
- by classes of service, up to 15
- by departments, up to five input areas
- by individually specified mailboxes, up to 10 input areas (more can be backed up using the wildcards '+' and '_')

For services, one of the following criteria may be used:

- all services on the system
- by service ID, up to 30 input areas (more can be backed up using the wildcards '+' and '_')

Backing up all users

Introduction The selective backup All option backs up all mailboxes on the system.

Labeling backup tapes During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level You can perform a selective backup of all users from the System Administration level only.

Procedure To perform a selective backup of all users, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press the Space Bar, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select All, and press the Tab key.
6	Enter the appropriate label for this selective backup.
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.

Step	Action
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up individual users

Introduction

The selective backup Individual option allows you to select specific mailboxes for backup by mailbox number.

Up to 10 individual mailbox input areas are provided, but the actual number of mailboxes may be much larger with the use of wildcards ('+' and '_').

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level

You can perform a selective backup of specified users from the System Administration level only.

Procedure

To perform a selective backup of specified individual users, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press the Space Bar to select it, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select Individual, and press the Tab key.
6	Enter the mailbox numbers for all individual mailboxes to back up. Use wildcards '+' and '_' to specify more than 10 mailboxes. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users in a specified volume

Introduction

The selective backup volume option backs up all users in the specified volume. As many volumes may be specified as are on the system.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level

You can perform a selective backup of specified volumes from the System Administration level only.

Procedure

To perform a selective backup of specified volumes, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select Volume, and press the Tab key.
6	Enter the volume numbers to be backed up.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users assigned to a particular class of service

Introduction The selective backup Class of Service option backs up selected classes of service. Up to 15 classes of service may be specified.

Recommendation It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level You can perform a selective backup of selected classes of service from the System Administration level only.

Procedure To perform a selective backup of selected classes of service, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this backup.
5	Use the arrow keys or space bar to move to COS (class of service) and press Tab.
6	Enter a list of class of service numbers to be backed up.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users in a specific department

Introduction

The selective backup Department option backs up all specified departments. Up to five departments may be specified, but the actual number of specified departments may be much larger with the use of wildcards ('+' and '_').

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level

You can perform a selective backup of selected departments from the System Administration level only.

Procedure

To perform a selective backup of selected departments, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this backup.
5	Use the arrow keys or Space Bar to select Dept, and press Tab.
6	Enter the department numbers to be backed up. Use wildcards '+' and '_' to specify more than 10 wildcards. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all multimedia services

Introduction The selective backup All option backs up all multimedia services.

Recommendation It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Administration level You can perform a selective backup of all multimedia services from the System Administration level only.

Procedure To perform a selective backup of all multimedia services, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Services, press the Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the arrow keys or Space Bar to move to All.
6	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.

Step	Action
7	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
8	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
9	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up selected individual multimedia services

Introduction

The selective backup Individual option backs up all specified multimedia services. Services are specified by service ID. There are 30 input areas for specified services, which can be expanded with the use of '+' and '_' wildcards.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Administration level

You can perform a selective backup of selected multimedia services from the System Administration level only.

Procedure

To perform a selective backup of all multimedia services, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Services, press the Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the arrow keys or space bar to select Individual, and press Tab.
6	Enter the numbers for service ID for all services to be backed up. Use wildcards '+' and '_' to specify more than 10 wildcards. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 16-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Section D: Partial backups to disk

In this section

Performing a partial backup to disk 16-40

Performing a partial backup to disk

Introduction

Backups to disk are only partial backups as the Voice and Data backup option is not allowed for user volumes. The backups options are Voice and Data for the system volume, and Data for user volumes.

Administration level

You can perform a partial backup from disk from a selective backup from the System Administration level only.

Procedure

To perform a partial backup to disk, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the arrow on the volume you want to backup and press <Space bar> to select it.
4	Enter an appropriate label for this backup.
5	Press [Backup to Disk]. **Result:** The Disk to Disk Backup screen appears.
6	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 16-42.
7	Do you want to continue with the backup? • If yes, press [OK to Start Backup] to initiate the backup. **Result:** The Backup status screen appears. • If no, press [Cancel] to return to the Disk to Disk backup screen.

Section E: Scheduled backups

In this section

Scheduling the backup for a later time 16-42
Deleting a scheduled backup 16-45

Scheduling the backup for a later time

Introduction

The Schedule Backup screen allows you to schedule the backup frequency (daily, weekly, or monthly) and start time for your backup to occur. This allows you to schedule a backup for which you do not need to be present.

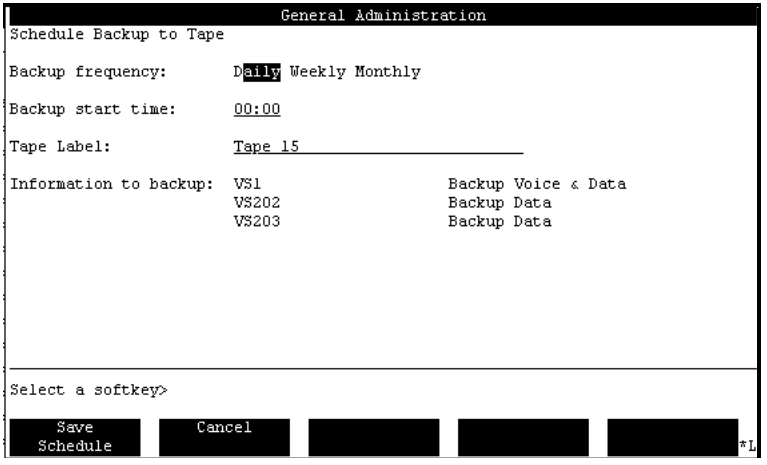
> **ATTENTION**
>
> Do not schedule important backups between 1:00 a.m. and 5:00 a.m. when important system audits occur. Do not schedule a backup if more than one tape is required.

Administration level

You can schedule a backup from the System Administration level only.

The Schedule Backup screen

This is the Schedule Backup screen.



Field descriptions

This table describes fields in the Schedule Backup screen.

Backup frequency	
Description	This field determines how often scheduled backups occur.
Default	Weekly
Valid options	Daily, Weekly, Monthly
Weekly	
Description	This field determines on which day of the week weekly backups occur.
Conditions of display	This field is displayed if the backup frequency is Weekly.
Default	Sun
Valid options	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Day of Month	
Description	This field determines on which day of the month monthly backups occur.
Conditions of display	This field is displayed only if the backup frequency is Monthly.
Default	1
Valid range	0 to 31
Backup start time	
Description	This is the time of day at which scheduled backups begin.
Default	00:00
Valid range	00:00 to 23:59

Tape label	
Description	This is the label that is given to the backup tape.
Default	Blank

Information to backup	
Description	This field displays the volumes you have selected to back up, or the criteria specified for a selective backup.

Procedure

To schedule a backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the cursor on the volumes and selective backups you want to back up and press <Space Bar> to select them.
4	Press [Backup to Tape] or [Backup to Disk].
5	Press [Schedule Backup].
6	Move the cursor to the required backup frequency (daily, weekly, or monthly) and press Return. **Result:** For weekly backups, the screen displays the days of the week; for monthly backups, the screen displays a prompt for the date on which the backups will occur.
7	For weekly backups, choose the day on which the backup will occur. For monthly backups, enter the required date.
8	Enter the backup start time.
9	Do you want to save the schedule? • If yes, press [Save Schedule]. • If no, press [Cancel] to return to the Volume and Selective Backup screen.

Deleting a scheduled backup

Introduction

The View/Delete Backup Schedule screen displays the currently scheduled backups. The screen is read-only and displays the current settings of the backup schedule, including the type of backup (to disk or tape), frequency of backup, start time, backup selection, and backup options.

Administration level

You can delete a previously scheduled backup from the System Administration level only.

Procedure

To delete a previously scheduled backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Press [View/Delete Schedule]. **Result:** The View/Delete Backup Schedule screen appears.
4	Press [Cancel Schedule]. **Result:** The schedule is deleted and you are returned to the Volume and Selective Backup screen.

Section F: Backup maintenance

In this section

Checking the status of a backup 16-48
Cleaning/maintaining the tape drive 16-52

Checking the status of a backup

Introduction

The Backup Status screen displays the current status of a backup, if one is in progress. The screen displays the time at which the backup started, time remaining for backup completion, volumes being backed up, selective backup criteria, and current progress of the backup. Time remaining will not be shown if selective backup was chosen.

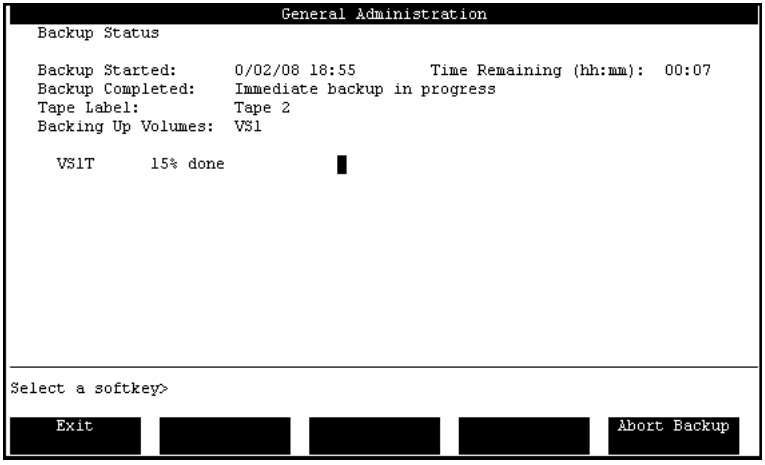
Exceptions

If you are performing a partial backup (Data) of a volume, there is an intermediate step in the backup process that will be reported in the status screen.

VS901T is used as a partial backup of VS202T, VS203T, VS204T, and VS205T. Text files are first copied to VS901T and then copied from VS901T to tape. While files are being copied to VS901T, the tape drive will be inactive. The status of VS901T will be reported on the Backup status screen while the backup is occurring.

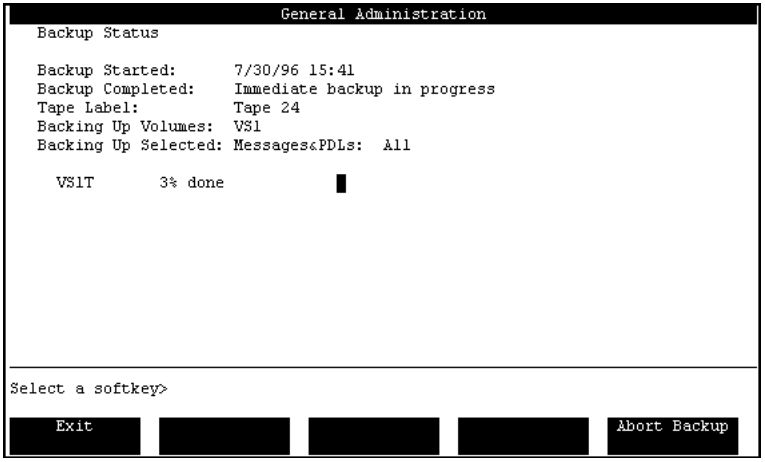
The Backup Status screen: partial backup

This is the Backup Status screen for a partial backup.



The Backup Status screen: selective backup

This is the Backup Status screen for a selective backup. There is no Time Remaining field.



Field descriptions

The following table provides field descriptions for the Backup Status screen.

Backup Started	
Description	The date and time the current backup started.
Date format	The date format is determined by the Date Format for Administration and Maintenance Reports field in the General Options screen.
Time Remaining	
Description	This is the time remaining to complete the backup, displayed in hh:mm.
Conditions of display	This field is not displayed if selective backup is chosen.
Backup Completed	
Description	This is the date and time at which the backup was completed. If the backup is still in progress, this field displays "Immediate backup in progress."
Tape Label	
Description	This is the label that was assigned to the tape.
Backup Volumes	
Description	If a full or partial backup is being performed, this field displays the list of volumes that are being backed up.
Backup Selected	
Description	If a selective backup is being performed, this field displays the criteria chosen to selected users and/or services for backup.

Administration level

You can check the status of the current backup from the System Administration level only.

Procedure

To check the status of a current backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Press [Backup Status]. **Result:** The Backup Status screen appears displaying information about the backup in progress, or about the last backup that was completed.
4	When you are finished viewing the status, you can exit the screen or abort the backup. • To exit the Backup Status screen, press [Exit]. • To abort a current backup, press [Abort Backup]. **Result:** You are returned to the Volume and Selective Backup screen.

Cleaning/maintaining the tape drive

Guidelines

Preventive maintenance of the tape drive involves periodic cleaning after every four to six hours of use.

Precautions

To ensure reliable tape drive performance, you should establish a regular cleaning schedule and observe the following precautions:

- Maintain a clean, dust-free environment within the temperature and humidity limits listed in the specifications of the Meridian Mail system.
- Keep all liquids away from the drive and tapes to prevent spills into the equipment.
- Exercise reasonable care when using and storing tape cartridges. Do not place cartridges on the Meridian Mail or Meridian 1 cabinets, or on the monitor of the system administrator's terminal.
- When a stored tape is moved to an environment with a greatly different temperature, allow the tape to slowly reach room temperature before using it.
- Do not touch the tape surface.

Reference

For detailed procedures on cleaning and maintaining the tape drive, see the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Section G: Restoring information from a Selective backup

In this section

Overview 16-54

Restore from Selective backup 16-56

Overview

Introduction

This section provides information on restoring from a Selective backup.

Description

The Selective Restore feature allows for an online restore of users' messages, individually specified Personal Distribution Lists (PDLs), or multimedia services. An entire mailbox is not restored, only the messages and PDLs for an existing mailbox. When restoring a user's messages and PDLs, the user is locked out of his or her mailbox until the restore is complete.

Restoring messages and PDLs

In restoring both messages and PDLs, if one already exists, it is not overwritten. For VMUIF users, no message will be restored to a mailbox once it is full. For MMUIF users, all messages are restored unless the Call Answering Blocking Factor is set.

Call Answering Blocking Factor limits the number of call answering messages that can be deposited in a mailbox once the number of messages in the mailbox exceeds the mailbox storage limit.

Restoring multimedia services

Restoring multimedia services can be done by service ID, or by restoring all services.

Restore exceptions

Data not restored from a selective backup includes mailbox configuration such as passwords, auto-login, storage limits, login status, and other data kept in the user's profile.

The More Detail screen

The Restore from Selective Backup More Detail screen provides a summary of the data backed up on a backup tape. The More Detail screen is accessed by the [More Detail] softkey in the Selective Backup and Restore screen.

Reference

For information on Full and Partial restores, see Chapter 6, “Restore system from backup,” in the *System Installation and Modifications Guide* (NTP 555-7001-215).

Restore from Selective backup

Introduction

The Selective backup option allows you to restore messages, PDLs, and multimedia services. This procedure allows you to select to restore none, all, or individual messages, PDLs, and multimedia services.

If you choose None, then nothing for that option will be restored. If you choose All, then everything for that option will be restored. If you choose Individual, then the system displays a list of the available Individual options from which to select. If you require more information about your restore tape, when in the Selective Restore screen, press [More Detail].

Administration level

You can restore from a selective backup from the System Administration level only.

Procedure

To restore from a selective backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Restore from Selective Backup. **Result:** The Restore from Selective Backup screen appears and prompts you to insert the restore tape in the tape drive.
3	Insert the tape in the tape drive, and press [OK to Read Tape]. **Result:** The tape drive retensions the tape. This takes approximately three to four minutes. Once the tape is retensioned, the screen displays the tape label and creation date. **Note:** If you require more information about the restore tape that you are using, press [More Detail] which will present a more detailed summary of the criteria used to perform the initial backup.

Step	Action
4	Use the arrow keys or space bar to select one of None, All, or Individual for Messages and PDLs, and press Tab. If you choose Individual, enter the mailbox(es), then select Yes or No for each of the Mailboxes, to restore messages or not respectively, and enter the PDL numbers you want to be restored.
5	Use the arrow keys or Space Bar to select one of None, All, or Individual for Services, and press Tab. If you choose Individual, then enter the Service IDs that you want restored.
6	Once you have selected all the required restore options, press [Restore]. **Result:** The system begins to read the requested data from the tape and transfer it to disk. Status information is displayed as % complete in the Status field. **Note:** When the restore is finished, a summary line will show the number of successes and failures for both mailboxes and services.
7	Do you want to perform another restore? • If yes, repeat steps 3 to 7. • If no, go to step 9.
8	Press [Exit] to return to the General Administration screen.

Chapter 17

Password and system time changes

In this chapter

Overview	17-2
Changing the system administrator password	17-3
Changing the customer administrator password	17-5
Setting the minimum password length for all administrator passwords	17-7
The AdminPlus Download password	17-8
Changing the system time	17-10

Overview

Introduction

This chapter describes

- how and how often to change the Administrator password and the AdminPlus Download password
- how to set the minimum length for the System Administrator passwordss
- how to change Meridian Mail's system time setting

Changing the system administrator password

Introduction

When the Meridian Mail system is first installed, you are given a default system administrator password (adminpwd). When you log on for the first time using this default password, you are prompted for a new password.

Administration level

You can change the system administrator password from the System Administration level only.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is set in the General Options screen. See "Setting the minimum password length for all administrator passwords" on page 17-7. The default length is six characters. It is recommended that your administration password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the system administrator password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change System Administrator Password. **Result:** You are prompted to enter the existing system administrator password.

Step	Action
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new administrator password.
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Reenter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Changing the customer administrator password

Introduction

When the Meridian Mail system is first installed, you are given a default customer administrator password (custpwd). When you log on for the first time using this default password, you are prompted for a new password.

Administration level

You can change the customer administrator password from both the System and Customer Administration levels.

In both cases, you must go through the General Administration Menu to reach the option to change the password.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is set in the General Options screen. See “Setting the minimum password length for all administrator passwords” on page 17-7. The default length is six characters. It is recommended that your administration password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the customer administrator password, follow these steps.

Starting Point: The Main Menu or the Customer Administration Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change Customer Administrator Password. **Result:** You are prompted to enter the existing customer administrator password.
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new administrator password.
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Enter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Setting the minimum password length for all administrator passwords

Introduction

Longer passwords generally offer higher system security. At least seven characters in length is a minimum recommendation. The minimum length you set here will be applied when system administrator and customer administrator passwords are changed.

Default minimum password length

The default minimum password length is 6 characters, and the maximum length is 16 characters.

Administration level

You can change the minimum administrator password length from the System Administration level only.

Procedure

To check or change the current minimum administration password length setting, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select General Options. **Result:** The General Options screen appears.
3	Cursor down to the Minimum Admin Password Length field.
4	Enter the new Minimum Admin Password Length, and press <Return>. The number must be a value between 6 and 16.
5	When you have entered the new value, press <Save>. **Result:** The new Minimum Admin Password Length is recorded and you are returned to the General Options menu.

The AdminPlus Download password

Introduction

The AdminPlus Download password allows Meridian Mail Reporter to download data from the system. This password must match the OM password on the Meridian Mail Reporter side before data can be downloaded. Both passwords must be set up when the system is installed as the default values will not allow the download to take place.

Note: This capability is only available if AdminPlus is an installed feature.

Administration level

You can change the AdminPlus Download password from the System Administration level only.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is 1 character, and the maximum length is 16 characters. It is recommended that your AdminPlus password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the AdminPlus password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change AdminPlus Password. **Result:** You are prompted to enter the existing system administrator password.

Step	Action
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new AdminPlus password.
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Enter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Changing the system time

Introduction

The Meridian Mail system gets its time from the Meridian 1. It receives time stamps passed from the switch at regular intervals. However, you can set up your Meridian Mail database while the link to the switch is down. If you will be configuring the database when the link is not operational, you will have to set the system time on the Meridian Mail side. Then, once the link is up, the switch time will override the Meridian Mail time.

Administration level

You can change the system time from the System Administration level only.

Procedure

To change the system time, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change System Time. **Result:** You are prompted to enter the date and time.
3	Enter the date and time, and press <Return>. **Result:** The clock is synchronized to the clocking signals from the network, the time is recorded, and the General Administration screen is redisplayed.
4	When you have set the system time, press <Exit>.

Chapter 18

Dialing translations

In this chapter

Overview	18-2
Section A: Introduction to dialing translations	18-3
Section B: How dialing translations work	18-17
Section C: Setting up network dialing prefixes and local defaults	18-29
Section D: Setting up translation tables	18-43
Section E: Sample datafills	18-69
Section F: Troubleshooting dialing translations	18-75

Overview

Introduction

This chapter introduces dialing translations as a concept and the ways that you, as the system administrator, can plan and set up dialing translation defaults and translation tables, if necessary.

Meridian Mail users do not directly access dialing translations. Taking the features and requirements of the system into consideration, the administrator needs to examine how private or public network numbers are dialed. Various features then use dialing translations to produce dialable numbers.

In the chapter, you will find explanations of what translations are, how they function, and when they are required. In addition, this chapter contains procedures that guide you through the administration of dialing translations.

Administration level

You can configure dialing translations from the System Administration level only.

Section A: Introduction to dialing translations

In this section

Overview	18-4
Dialing translations	18-5
Default dialing prefixes and local system defaults	18-7
When default dialing translations defaults are required	18-10
Translation tables	18-12
When translation tables are required	18-14

Overview

Introduction

This section introduces the concept of dialing translations and the ways in which they are implemented.

This section discusses the two main parts of dialing translations: dialing translation defaults and translation tables.

Dialing translations

Description

Dialing translations are the means by which Meridian Mail transforms a number into a dialable directory number (DN). For instance, translation determines how to dial a DN depending on whether a number is a local, national, international, or ESN.

How translations are used

Users of Meridian Mail do not directly use translation. Rather, certain features use dialing translations in order to generate a dialable DN to call back:

- The system administrator uses default dialing prefixes to handle normal situations for local, national, international and (if they exist) ESN calls.
- Exceptional situations, such as calls to other area codes that are still considered local calls, use translation tables.

Example

For example, if a caller requests that a fax be sent to 214-555-1234 (a long distance number), this number must be translated into a DN that can be dialed from your system. In this case, the dialable DN must include the long distance dialing prefix. If your system dials “91” to place long distance calls, then the resulting DN will be 91-214-555-1234.

Features that use dialing translations

The following features use dialing translations:

- Fax on Demand
  - For example, a user calls Meridian Mail, enter a fax number without a prefix and wait for the fax to call back.
- AMIS Networking
  - For example, a user receives a message from a remote AMIS site and the number is included in the message header. The number must be translated to use the Reply feature to call back.

- External CLID
  - For example, CLID collects the caller's number from the switch. Meridian Mail translates the number, and it is announced in a message to you with the prefixes included, ready to dial out.

Outcalling does *not* use translations

Default dialing prefixes are not required for outcalling (remote notification and delivery to non-user.) The numbers entered are already in a dialable format and, therefore, do not need to be translated for a callback.

Default dialing prefixes and local system defaults

Introduction

There are two levels to the translation process. The first level involves dialing translation defaults, which include default dialing prefixes and local system defaults. Both are used only under normal dialing conditions.

Default dialing prefixes

The system administrator must define four default dialing prefixes:

- local
- long distance
- international
- ESN

These prefixes are the dialing digits that are used to dial out of the switch to place local, long distance, international, and ESN calls using either the public network, the ESN network, or a combination of both.

Meridian Mail uses these prefixes to generate a DN that is understandable to the switch.

Local dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place a local call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place local calls. Typical examples of network dialing prefixes are 9 or 8 to access the public network.

To access a private ESN network is a little more complicated. You would typically dial 6 plus the digits needed to make a national call to the same local site. For instance, the area/city code of Manhattan is 212, so the prefix would be 61212.

Long distance dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place a long distance call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place long distance calls. Typical examples of long distance dialing prefixes are 91 or 81 in North America, or 90 or 80 in Germany, to access the public network, or 6 to access a private ESN network.

International dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place an international call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place international calls. Typical examples of international dialing prefixes in North America are 9011 or 8011 to access the public network, or 6011 to access a private ESN network.

An international dialing prefix in England, for example, is 900.

ESN dialing prefix

This is the prefix that is used by the system to access the private ESN network.

Local system defaults

Local system defaults identify the country and the area/city codes of the switch connected to your Meridian Mail.

You will fill out these fields to inform Meridian Mail of its location within the public network. This information is used by dialing translations to determine how to translate a number.

Country code

Identify the country code for your system. (For instance, it is 1 for the U.S.A. and Canada. It is 44 for England, 61 for Austria, and 86 for China.)

Local system defaults (cont'd)

Area/city code

Identify the area/city code for the local system.

The term "area/city code" is used to define either area code or city code. The two terms are used interchangeably.

Countries that use city codes should use this field for city codes, and countries that use area codes should use the field for area codes. However, if a country uses *both* area and city code for its dialing plan, the field should be used for *either* the area or city codes for the site in which the Meridian Mail is located.

When a number that includes an area/city code is provided by a caller for a fax callback delivery or by a user when replying to an AMIS message, it will be stripped out if it matches the code entered in the field.

Example

A caller requests that a fax item be sent (using callback delivery) to the DN 416-555-9911. The local system's area/city code is also 416. Therefore, the area code will be stripped out and the dialable DN will be 9-555-9911, where 9 is the network dialing prefix (for local calls).

When default dialing translations defaults are required

Description

The dialing translation defaults must be filled in before features like AMIS networking, Fax on Demand, and External CLID can be used.

The dialing translation defaults consist of

- default dialing prefixes

  This is where you specify the network access codes that are used by your system for placing local calls, long distance calls, international calls and ESN calls. These prefixes are needed to generate dialable DNs from

  - fax callback numbers
  - numbers contained in the headers of AMIS messages (so that local users can reply to AMIS messages)
  - numbers of external callers who left messages with users on your system
- local system defaults

  This is where you enter the country code and the area/city code of your Meridian Mail site. These codes are used to determine if the country or area/city code entered by a caller needs to be stripped out.

Scenario

In a Fax on Demand application, for example, a caller includes the country code and area/city code in the callback number he or she has entered.

Meridian Mail checks the values defined to see if the country and area/city codes specified in the callback number match the codes of the Meridian Mail system. If there is a match, the country and area/city codes which are not required, if any, for dialing purposes and are stripped out.

Example of the scenario

A caller enters 1-214-555-2222 as a callback number for a fax. The country code (1) and the area/city code (214) are the same as the one for the Meridian Mail system. Therefore these codes are not needed to dial the number.

Meridian Mail strips out the 1214, gets the network dialing prefix for local dialing (9), and generates the following dialable DN: 9-555-2222.

Translation tables

Concept

Translation tables are the second level of the translation process, after the dialing translation defaults.

These tables handle certain dialing exceptions that may not arise in your system. Therefore, translation tables will not be required by all systems.

For example, in a normal local dialing scenario, the area/city code (in North America, it is called the Numbering Plan Area or NPA) of the calling site is the same as the called site. A call in this situation would be handled by the dialing defaults.

However, there may be a dialing scenario where the area/city codes are different but the call is still considered local. A translation table would have to handle this case in order to determine that the call in question could be handled as local rather than as long distance.

The exceptional cases that require translation tables are outlined in “When translation tables are required” on page 18-14.

Restriction/ permission lists

Meridian Mail applies translation tables before checking restriction/permission lists.

Example

For example, a call to another area/city code is considered local, and the restriction/permission list applied to a Fax on Demand application allows only local calls.

If a translation table is not set up for this exceptional dialing scenario, the system will assume that the callback number is long distance (because the area/city code is different from the local site) and Meridian Mail will not deliver the fax (since the restriction/permission list does not allow delivery to long distance numbers).

Restrictions for AMIS and Fax on Demand

For more information on how restrictions and permissions interact with Fax on Demand and AMIS Networking, refer to the following NTPs: *Fax on Demand Application Guide* (NTP 555-7001-327) and the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242).

When translation tables are required

Description

Translation tables need only be defined if

1. some calls placed to the same area/city code as the local site are dialed differently than local (for example, long distance)
2. calls placed to different area codes are not dialed long distance

For example, if calls to some numbers in an area/city code are long distance, while calls to other numbers in that same area/city code are local, a translation table would be used to determine dialable DNs. This situation is normally dictated by the dialing plan of the local public network.

Translation tables for four exemplary cases

If any of the following situations occur in your system, you will have to define a translation table for each area/city code.

Type of dialing	To what area/city code?	Is the area/city code required in the DN?
Local dialing	Different	Required
Local dialing	Different	Not required
Long distance dialing	Same	Required
Long distance dialing	Same	Not required

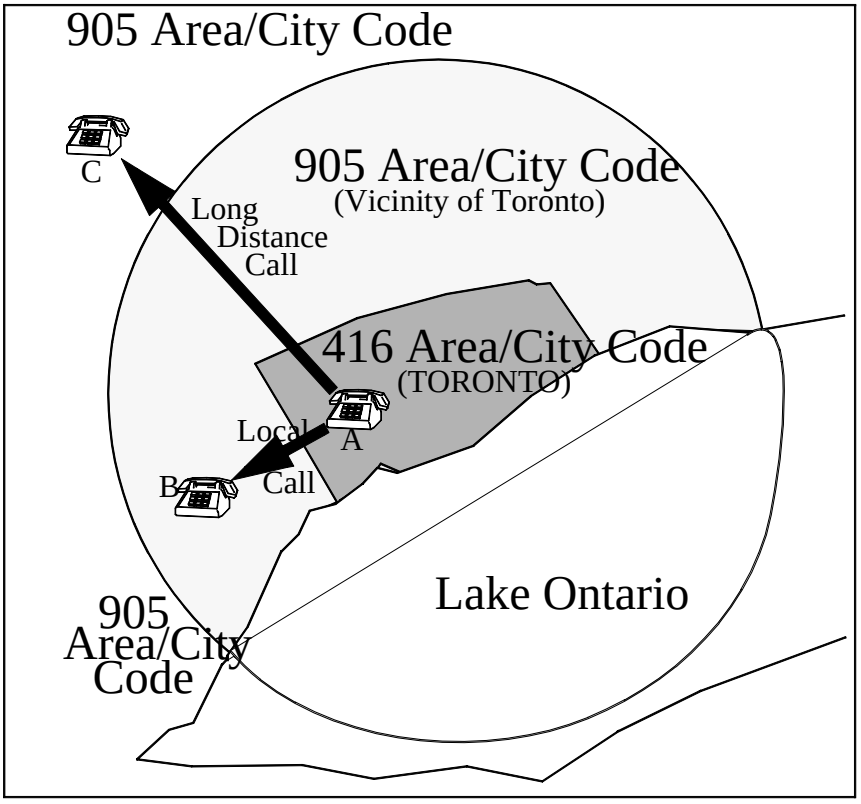
In all other dialing scenarios (such as long distance dialing to a different area/city code and local dialing to the same area/city code), the network dialing prefixes are used instead.

Example 1

For example, if a neighboring area code (905) contains both local and long-distance numbers, and a call to a local number in the 905 area needs a different number format than a call to a long-distance number in the 905 area, at least one translation table will be required.

The table determines on the basis of the local prefix which calls are local, and which are long distance.

Example 1 (cont'd) Consider the following example which shows the dialing plan of Toronto, Ontario, Canada.



You can see that both local (A→B) and long-distance (A→C) dialing is used depending on the location of the destination call.

A translation table must be defined to tell Meridian Mail which 905 numbers must be dialed as long distance and which ones must be dialed as local.

Section B: How dialing translations work

In this section

Overview	18-18
How Meridian Mail collects digits	18-19
How dialing translations translate numbers	18-22
How Meridian Mail uses the dialable number	18-27

Overview

Introduction

The dialing translation process occurs in three stages:

- input to the translation process (how DN digits are collected)
- the translation itself (how the collected DN is translated)
- output from the translation process (what happens to the translated DN)

This section will discuss each stage.

How Meridian Mail collects digits

Description

The format in which Meridian Mail requires a DN depends on the feature using dialing translations.

The three features using dialing translations are

- Fax on Demand
- AMIS Networking
- External Calling Line Identification (External CLID)

The following descriptions explain how each feature collects digits for translation.

Fax on Demand

When users call the Meridian Mail Fax on Demand service (VSDN), Meridian Mail prompts users for the number of their fax machine to which the fax will be sent.

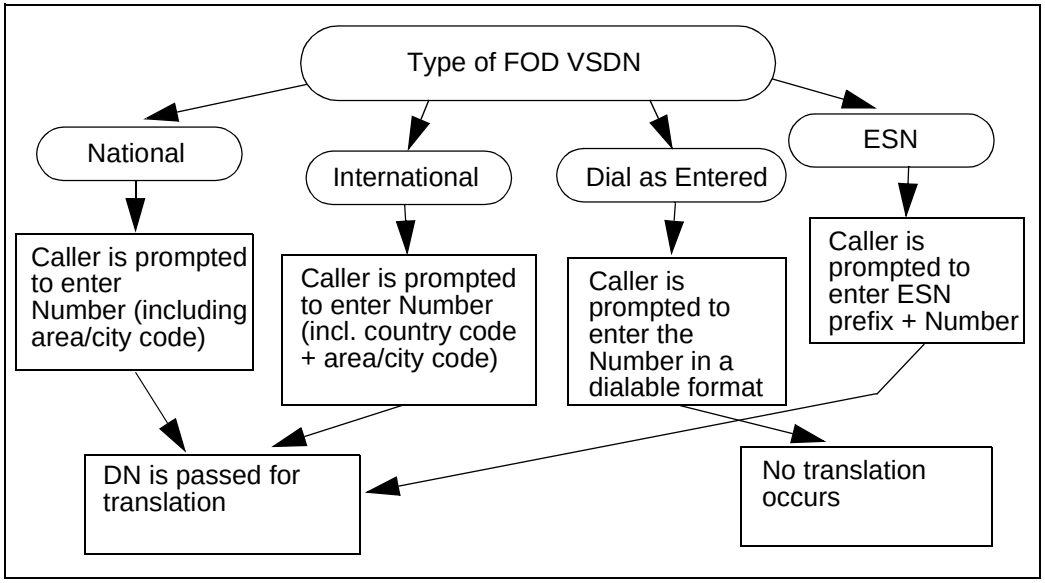
A session profile sets up the operational characteristics of the Fax on Demand service. Using the session profile, the Fax on Demand VSDN can be set up as national, international, dial-as-entered, or ESN.

This setup is done in the Treat Callback Number As field in the Session Profile screen for that VSDN.

Different prompts exist for each type of service. The prompts ask the user to enter the fax number in a particular format (national, international, dial-as-entered, or ESN.)

Digit collection for fax callback

The following diagram illustrates the different types of the Fax on Demand VSDN and what the caller is prompted for each type.


Type of FOD VSDN
National
International
Dial as Entered
ESN
Caller is prompted to enter Number (including area/city code)
Caller is prompted to enter Number (incl. country code + area/city code)
Caller is prompted to enter the Number in a dialable format
Caller is prompted to enter ESN prefix + Number
DN is passed for translation
No translation occurs

After the DN is passed for translation, the translation type depends on the type of FOD VSDN.

For more information about VSDNs, see Chapter 25, "The VSDN table" under Section E: Session profiles.

AMIS

AMIS collects digits for translation in two ways:

- When an AMIS message is received from a remote AMIS site, the number from that site (in an international, nondialable format) is included in the message.

  When the user replies to this message, or when the Meridian Mail system determines that the message cannot be delivered and generates a Non-Delivery Notification (NDN) to that remote system, the number must be translated into dialable DN before the remote system can be reached.

  Refer to the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242) for more details.

- When a message is sent to a Virtual Node AMIS site, the connection DN defined for that site must be translated into a dialable DN.

  Refer to the *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245) for more details.

In both AMIS cases, the number is translated as an international number.

External CLID

External CLID collects digits from the switch. When an external caller calls a user at the local system and leaves a message for the local user, the caller's number is passed to Meridian Mail by the switch. The *type* of this number (national, international, ESN, and so on) is also passed to Meridian Mail from the switch.

In order to make this number dialable, the External CLID feature translates the number to a dialable format using dialing translations. The type of translation depends on the number type received from the switch.

Suggestions for CLID

This feature must set the translation of the unknown calling number type to one of the following: local, long distance, international, or ESN. It means that the system administrator must be confident that all the unknown incoming calls are the same type (because all the unknown calls will be translated as though they were the same type).

If those unknown calls are of more than one type, the system administrator must either decide not to translate the number (to treat it as dialed), or not to collect the unknown numbers.

How dialing translations translate numbers

Introduction

Once the number has been captured (as explained in the previous section), dialing translations is applied to it.

The following flowcharts illustrate the way in which the translation is achieved by individual type.

Five translation types are available:

- international
- national
- local
- ESN
- dial-as-entered

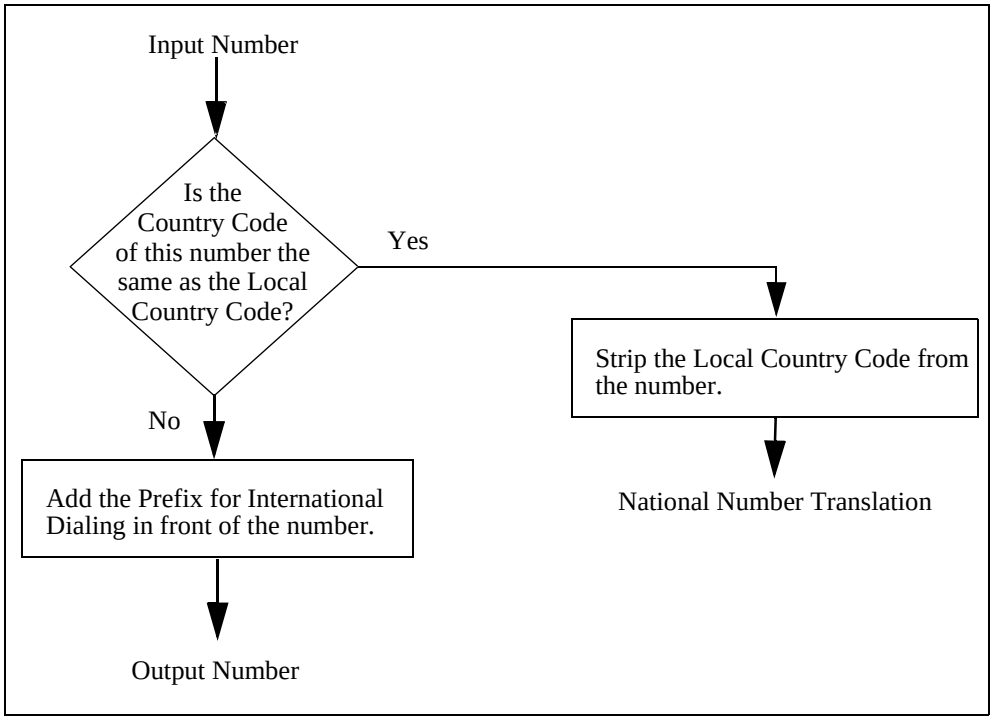
The translation type used depends on the type of number collected by the Fax on Demand, AMIS, or External CLID features. For instance, an international number will undergo an international translation, and so on.

International number translation

An international number is always in the format of

- country code + national significant number

It is translated in the following manner:

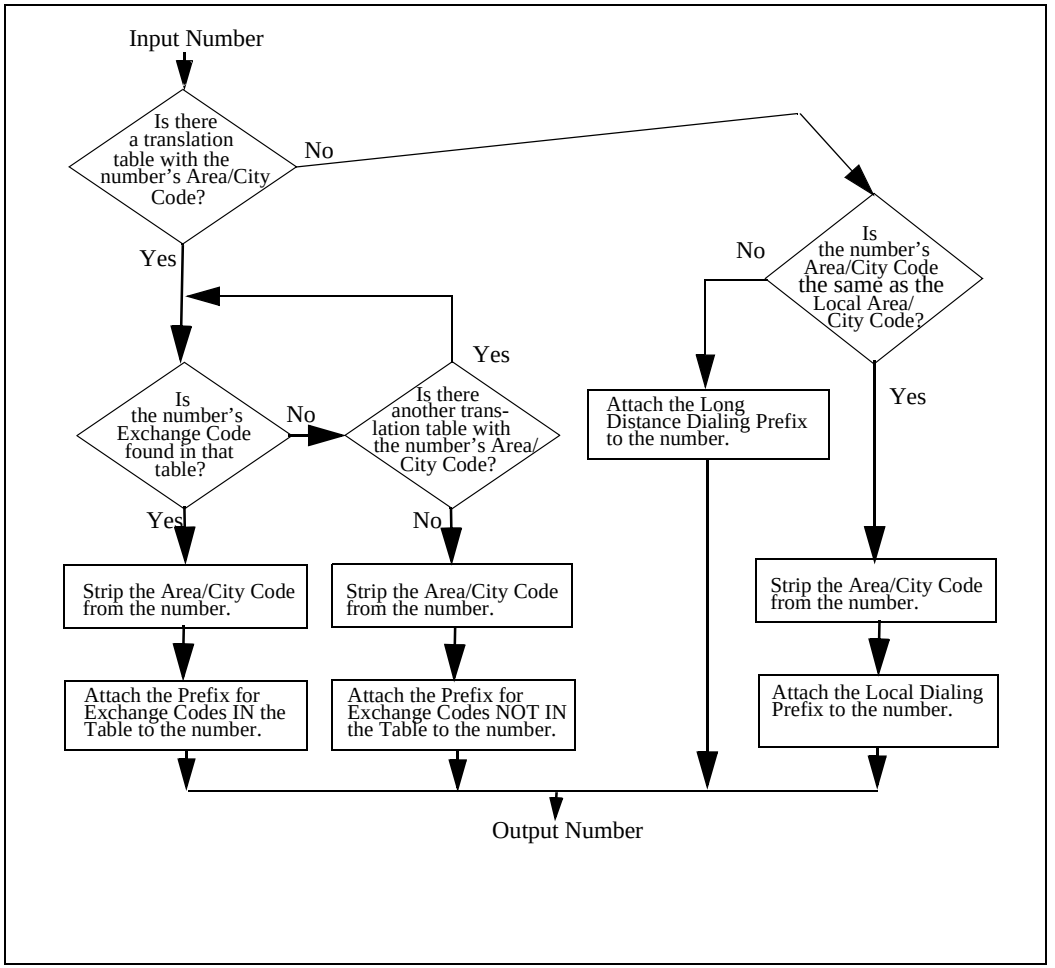

Input Number
Is the Country Code of this number the same as the Local Country Code?
Yes
No
Strip the Local Country Code from the number.
National Number Translation
Add the Prefix for International Dialing in front of the number.
Output Number

National number translation

A national number is always in the following format:

- area/city code + exchange code + station number

It is translated in the following manner:

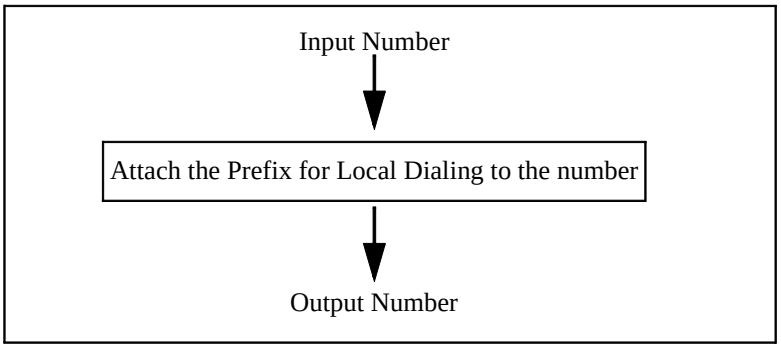

Input Number
Is there a translation table with the number's Area/City Code?
No
Yes
Is the number's Area/City Code the same as the Local Area/ City Code?
No
Yes
Is the number's Exchange Code found in that table?
No
Yes
Is there another trans-lation table with the number's Area/ City Code?
Yes
No
Attach the Long Distance Dialing Prefix to the number.
Strip the Area/City Code from the number.
Strip the Area/City Code from the number.
Strip the Area/City Code from the number.
Attach the Prefix for Exchange Codes IN the Table to the number.
Attach the Prefix for Exchange Codes NOT IN the Table to the number.
Attach the Local Dialing Prefix to the number.
Output Number

Local number translation

The local number is always in the following format:

- Local subscriber number (*without* country code or area/city code)

The translation proceeds as follows:



ESN number translation

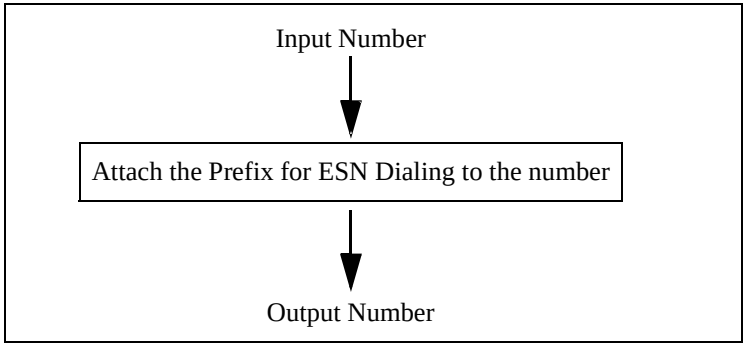
The ESN number can be in one of the following formats:

- a number on the ESN network
  - for example, 444-1000

    where 444 is the location code of the ESN switch, and 1000 is the DN at the ESN location
- any number dialable via the ESN network
  - for example, 1-212-555-1234

    where the entire number can be dialed via the ESN network by adding the prefix for ESN dialing in front of it

In both cases, the translation proceeds as follows:



Dial-as-Entered translation

The dial-as-entered number is always in the following format:

- Any string of digits

A dial-as-entered number is *not* translated. The number is assumed to be dialable exactly as it is specified (that is, containing all required prefixes and codes).

How Meridian Mail uses the dialable number

Introduction

Once the number is translated, it is returned to the feature that required the translation.

Fax on Demand

For Fax on Demand, the translated number will be checked against restriction/permissions for that VSDN.

If the number passes the check, Meridian Mail dials the number so that the requested fax can be delivered to the user. If the fax fails the restriction/permission check, the user requesting the fax will be informed that the number cannot be reached from that service and asked to enter another number.

AMIS

In AMIS, the translated, dialable number will be checked against AMIS restriction/permission lists. If the number passes the check, Meridian Mail uses the number to call the remote AMIS system so that AMIS Networking messages can be delivered to the system.

If the number fails the check (that is, it is restricted and Meridian Mail cannot dial the number), the AMIS message will not be delivered and a Non-Delivery Notification (NDN) will be sent to the sender of the message.

External CLID

In External CLID, the translated number is used for

- call sender

  The user places a call to the number.
- announcing the sender's number

  In the message header, or when the user uses call sender, or call reply.

When the user listens to a message from an external caller, the user will hear

- "From phone number: <digits>"

  where "digits" is the translated number

External CLID (cont'd) When the user requests a reply or call-sender to the caller, the number will be announced. When the user requests call sender, this translated number will be dialed so that the caller who left the number can be reached.

Note: Before being dialed, the number will also be checked against the restriction/permission list. Call sender will only continue if the number passes this check (that is, it is not restricted.)

Section C: Setting up network dialing prefixes and local defaults

In this section

Overview	18-30
Worksheet for default dialing prefixes and local system defaults	18-31
Dialing translation defaults screen	18-33
Configuring the default dialing prefixes and local system defaults	18-37
Sample datafills for dialing translation defaults	18-40

Overview

Introduction

This section explains how to set up and maintain dialing translation defaults for your system.

In addition to explanatory concepts and procedures, there are sample datafills to which you may compare your system and a worksheet to help you plan your dialing translations.

Worksheet for default dialing prefixes and local system defaults

Worksheet

You can use the following worksheet to plan default dialing prefixes and local system defaults.

Dialing Translation Defaults worksheet

Default Dialing Prefixes

Local Dialing: _____

Long Distance Dialing: _____

International Dialing: _____

ESN Dialing: _____

Local System Defaults

Local Country Code: _____

Local Area/City Code: _____

Dialing translation defaults screen

Introduction

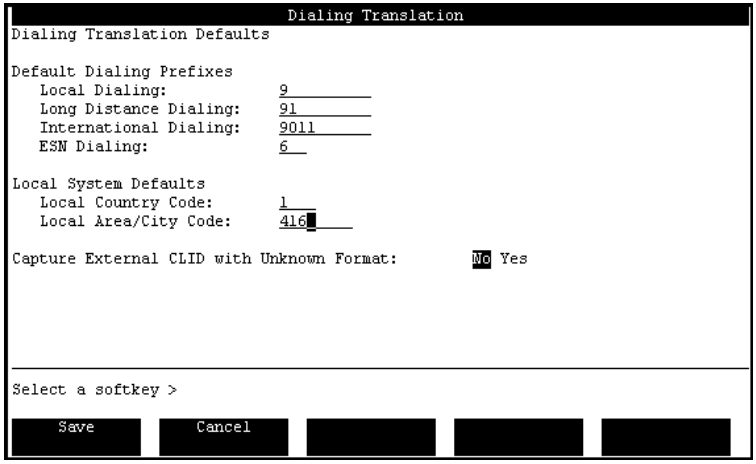
When you are ready to configure the default dialing prefixes and the local system defaults, you will need to access the dialing translation defaults.

Administration level

You can configure dialing translations from the System Administration level only.

The screen

The following shows an example of the Dialing Translation Defaults screen.



Field descriptions

The following table describes the fields in the Dialing Translation Defaults screen.

Local Dialing	
Description	This field specifies the prefix needed in front of a number when dialing it (and the number dialed is in the same area/city as the Meridian Mail system).
Minimum length	0 (zero characters)
Maximum length	10 characters
Valid characters	0-9, * (where * is a pause)

Long Distance Dialing	
Description	This field specifies the prefix used for long-distance dialing of public network numbers. Meridian Mail places this prefix in front on long distance DNs before placing a call (for example, National numbers with a different area/city code)
Minimum length	Zero characters
Maximum length	10 characters
Valid characters	0-9, * (* is a 3-second pause)

International Dialing	
Description	This field specifies the prefix used for international dialing of public network numbers. Meridian Mail places this prefix in front of international DNs (for example, DNs with a different country code)
Minimum length	Zero characters
Maximum length	10 characters
Valid characters	0-9, * (* is a 3-second pause)

ESN Dialing	
Description	This field specifies the prefix that needs to be attached to a number to access the ESN network. Meridian Mail places this prefix in front of ESN DNs.
Minimum length	Zero characters
Maximum length	Three characters
Valid characters	0-9, * (* is a 3-second pause)

Local Country Code	
Description	This field defines the country code of the local system.
Minimum length	Zero characters
Maximum length	Four characters
Valid characters	0-9, * (* is a 3-second pause)

Local Area/City Code	
Description	This field defines the area/city code of the local system.
Minimum length	0
Maximum length	Eight characters
Valid characters	0-9

Capture External CLID with Unknown Format	
Description	This field specifies whether to capture an external caller's number (External CLID) if that caller's format is unknown. This capability may be necessary in the case where the numbers received by Meridian Mail from the switch are in an unknown format.
Default	No
Feature dependency	This field appears only on systems with either AML or DIAL.

Default Translation for CLID with Unknown Format	
Description	This field specifies how the external caller's number (External CLID) of unknown type is translated if it is captured. Setting this field to Local, National, International, or ESN results in the External CLID being translated as though the DN were Local, National, International, or ESN, respectively.
Default	None (that is, no translation is performed on the number)
Field status	This field appears only if Capture External CLID with Unknown Format is set to Yes.

Configuring the default dialing prefixes and local system defaults

Introduction

Once you have identified the ways that your system makes external calls through a private or public network, or a combination of both, you are ready to configure your dialing translation defaults which include the default dialing prefixes and the local system defaults.

Administration level

You can configure dialing translations from the System Administration level only.

Procedure

To configure the default dialing prefixes and the local system defaults, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose General Administration. **Result:** The General Administration menu is displayed.
2	Choose Dialing Translation. **Result:** The Dialing Translation menu is displayed.
3	Choose Dialing Translation Defaults. **Result:** The Dialing Translation Defaults screen is displayed.
4	Define the Prefix for Local Dialing. **Note:** For more information, see “Local dialing prefix” on page 18-7.
5	Define the Prefix for Long Distance Dialing. **Note:** For more information, see “Long distance dialing prefix” on page 18-8.
6	Define the Prefix for International Dialing. **Note:** For more information, see “International dialing prefix” on page 18-8.

Step	Action

7 Define the Prefix for ESN Dialing.

IF your system is	THEN
connected to an ESN network	define the prefix.
not connected to an ESN network	leave the field blank.

Note: For more information, see “ESN dialing prefix” on page 18-8.

8 Define the local Country Code.

Note: For more information, see “Local system defaults” on page 18-8.

9 Define the local Area/City Code.

IF	THEN
your MM system is located in an area code	enter that area code.
your MM system is located in a city code	enter that city code.
your country does not have either area or city codes	leave this field blank.

Note: For more information, see “Local system defaults” on page 18-8.

10 Does your system have AML or DIAL?

- If yes, continue with the next step.
- If no, go to step 13.

Step	Action
11	Do you want to capture External CLIDs that are of an unknown type? • If yes, set the “Capture External CLID with Unknown Format” field to Yes. • If no, set the “Capture External CLID with Unknown Format” field to No. Go to step 13.
12	Set the “Default Translation for CLID with Unknown Format” field so that all numbers with an unknown call type will be translated as though they were all of one format.

IF all numbers of unknown format are	THEN set the field to
international	International.
national	National.
ESN	ESN.
not to be translated	None.
of various different formats	Nothing. Do not use this field. Return to step 11, and select No.

13	Do you want to save the screen? • If yes, press the [Save] softkey. • If no, press the [Cancel] softkey.

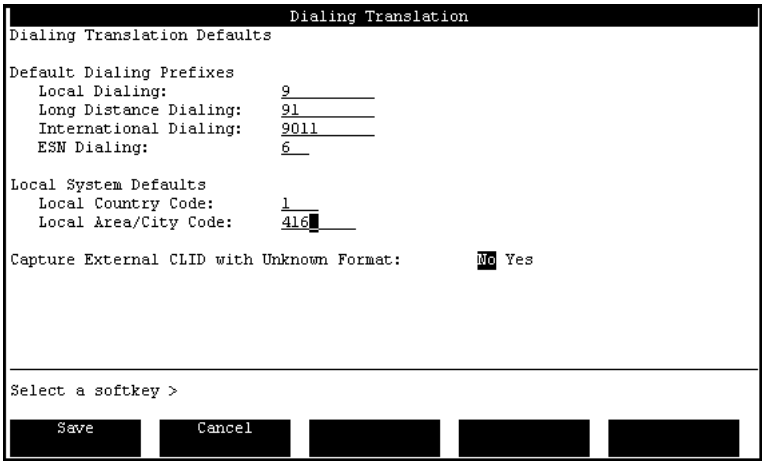
Sample datafills for dialing translation defaults

Introduction

You may compare the following sample datafills of dialing translation defaults to handle different methods of dialing (private versus public network).

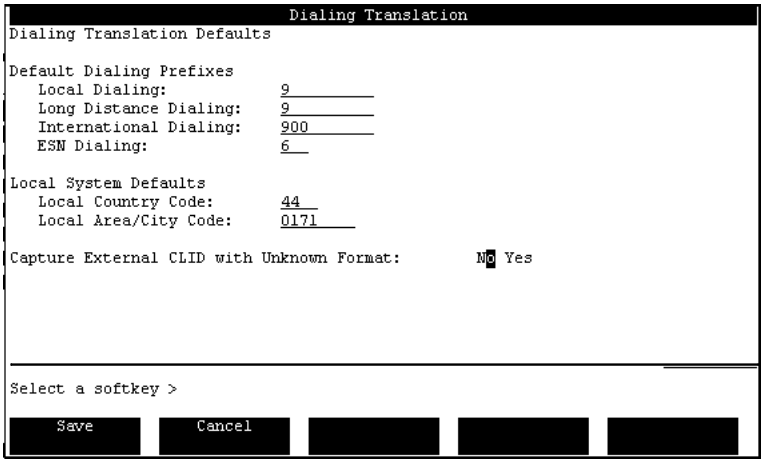
Defaults screen for North America

The screen below illustrates a standard dialing plan situation in Toronto, Ontario, Canada, where the country code is 1and the area code is 416. In this example, the digit 6 accesses the ESN network.



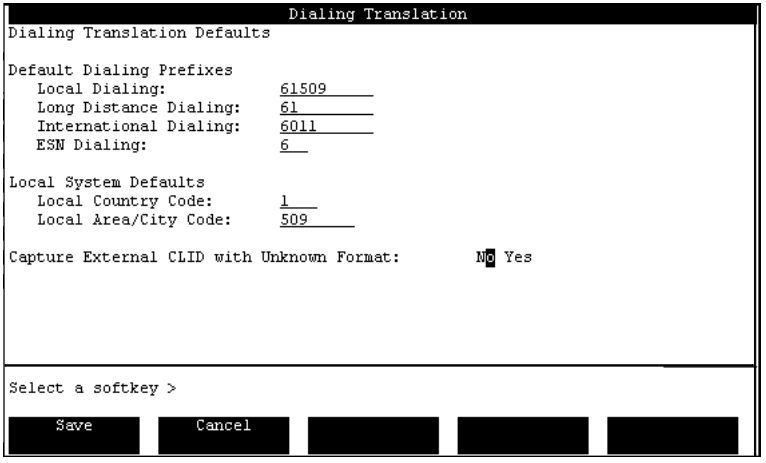
Defaults screen for England

The screen below illustrates a standard dialing plan situation in England where the country code is 44. In this example, the digit 6 accesses the ESN network.



All ESN screen

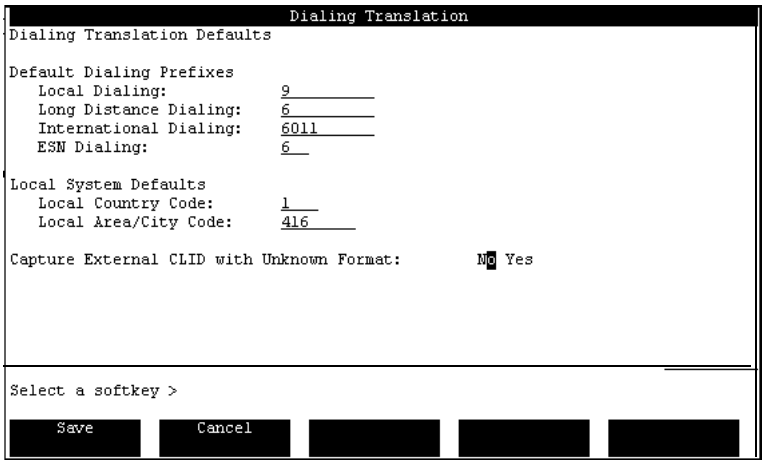
If your system makes all calls though a private network, then your network dialing prefixes would all begin with the access to the ESN network. In this example, the digit 6 accesses the ESN network.



Mixture of ESN and public screen

If your system makes calls through a combination of private and public networks, then you may use a combination of access prefixes.

This example illustrates the datafill for a system in which the local calls are dialed on the public network, but long distance and international calls are dialed on the ESN network.



Section D: Setting up translation tables

In this section

Overview	18-44
Identifying translation table requirements	18-45
Identifying translation tables required on your system	18-48
Local dialing to a different area/city code (area/city code required)	18-52
Local dialing to a different area/city code (no area/city code required)	18-56
Long distance dialing to the same area/city code (area/city code required)	18-59
Long distance dialing to the same area/city code (area/city code not required)	18-61
The View/Modify Translation Table screen	18-62
Configuring translation tables	18-64
Deleting translation tables	18-67

Overview

Introduction

This section guides the system administrator through all aspects of translation tables.

First, this section explains and illustrates the differences between normal dialing scenarios (ones that do not require translation tables) and exceptional dialing scenarios (ones that require translation tables). In so doing, this section demonstrates when translation tables are needed.

Second, this section explains in detail some of the exceptional dialing scenarios to provide you with a better idea of what each scenario is, how to handle each one, and how to handle any other exceptions that may occur.

Finally, this section contains procedures for adding, modifying, and deleting translation tables on the Meridian Mail, as well as field descriptions for those tables.

Identifying translation table requirements

Introduction

Not all systems require translation tables, so you must first identify if there is a need for a table on your system.

If the following cases are the only local and long distance scenarios that take place, you will not have to create any translation tables. Meridian Mail will use the prefixes that are defined in the Dialing Translation Defaults screen to perform all the translations required.

Normal dialing cases

All DNs with the same area/city code as the local site are treated as local calls.

All DNs with a different area/city code to the local site, are treated as long-distance.

Meridian Mail assumes that all the numbers in the local area/city code are dialed with the local dialing prefix and *without* the local area/city code (in other words, with a format such as 9-xxx-xxxx).

Meridian Mail also assumes that all numbers in area/cities other than the local area/city are dialed with the long distance dialing prefix and with the area/city code of the number (in other words, with a format such as 6 [xxx]-xxx-xxxx).

If these two statements are true for your system, you do not need to define any translation tables. Otherwise, if either or both of these statements are not always true for your system, then translation tables will have to be defined for the exceptional cases.

Dialing cases requiring translation tables

The following table shows examples of the exceptional dialing scenarios that require translation tables.

Case	Is area/city code in called DN same as or different than the local site's area/city code?	Called Area Is	DN Format needs to be
1	Different	Local	Local dialing prefix + area/city code + local number
2	Different	Local	Local dialing prefix + local number
3	Same	Long Distance	Long distance dialing prefix + area/city code + local number
4	Same	Long Distance	Long distance dialing prefix + local number

Cases 1 and 2

Local dialing to another area/city code

For cases 1 and 2, you need to define those instances in which calls to certain exchanges in *another* area/city code (other than your system's) are considered local.

These are exceptional scenarios and require translation tables.

In the translation table, specify either the exchange codes to which a call is considered local or the exchange codes to which a call is considered long distance.

Use the method that results in entering the smaller number of exchange codes. For example, if 200 exchange codes in the area/city code are considered local and 12 are long distance, enter the exchange codes to which dialing is considered long distance.

Cases 3 and 4

Long distance dialing to the same area/city code

For cases 3 and 4, define those instances in which a call to certain exchanges in the *same* area/city code as your system's area/city code are considered long distance.

These cases are also exceptional scenarios, and require translation tables. A translation table allows you to define which exchanges in your area/city are considered local and which exchange codes are considered long distance.

In the translation table, enter either the exchange code to which calls are considered long distance or local (depending on which method results in entering the lesser number of exchange codes).

Creating multiple tables

If more than 120 exchange codes are required for one area/city code, create another table for the area/city code. A number of tables that are created for the same area/city code can be considered a "joint" table. If this is the case, the Prefix for exchange codes *not* in the table field must be identical for all tables that are created for the same area/city code.

Other dialing exceptions

Other dialing exceptions may exist, for example, dialing to the local area/city with a local dialing prefix *and* with the local area/city code in the number dialed. You would also need to define translation tables for these exceptions.

Identifying translation tables required on your system

Introduction

A translation table is needed for an area/city code if calls placed from your system to that area/city code are made in one of the ways that are not supported by the dialing translation defaults. (The scenario where defaults alone support dialing translation is described in “Identifying translation table requirements” on page 18-45.)

Area/city code

A translation table is defined for an area/city code. You should have a good idea of the exchange codes and the two prefixes for the table before you define the table.

Exchange codes

You should identify the exchange codes for the translation table before you identify the prefix for the exchange codes in the table and the prefix for the exchange codes not in the table. This is because depending on which exchange codes you define in the table (they may be considered local or long distance), these prefixes will change.

Prefix for exchange codes in the table

For those exchange codes that are defined in the table, this prefix will be used by the system to dial out of the switch and place the call. Therefore, depending on the scenario, this prefix will either be for local dialing or long distance dialing. The prefix is needed to generate a dialable DN that is understood by the switch.

Prefix for exchange codes *not* in the table

For those exchange codes *not* defined in the table (or any other table for this area/city code) that belong to the area code to which the table applies, this prefix will either be for local dialing or long distance dialing. This prefix is needed to generate a dialable DN that is understood by the switch.

Prefixes for exchange codes - North American example

This table illustrates the format of the prefixes for exchange codes in, and *not* in, the translation table of a North American dialing plan. Remember that you can find these same examples in the scenarios described in more detail on the following pages.

Dialing scenario	Prefix for exchange codes in table	Prefix for exchange codes NOT in table
1. Local dialing to a different area/city code (area/city code required in DN).		
Exchange codes defined in table are considered local.	Y-NPA (9-905)	P-NPA (9-1-905)
Exchange codes defined in table are considered long distance.	P-NPA (9-1-905)	Y-NPA (9-905)
2. Local dialing to a different area/city code (no area/city code).		
Exchange codes defined in table are considered local.	Y (9)	P (9-1)
Exchange codes defined in table are considered long distance.	P (9-1)	Y (9)
3. Long distance dialing to same area/city code (area/city code required in dialing).		
Exchange codes defined in table are considered long distance.	P-NPA (9-1-214)	Y (9)
Exchange codes defined in table are considered local.	Y (9)	P-NPA (9-1-214)
4. Long distance dialing to same area/city code (area/city code required in dialing).		
Exchange codes defined in table are considered long distance.	P (9-1)	Y (9)
Exchange codes defined in table are considered local.	Y (9)	P (9-1)

- Y is the local dialing prefix (9, 8, or 6).
- P is the long distance dialing prefix (91).
- NPA is the Numbering Plan Area (area code).

Translation table worksheet

You can use the following worksheet to plan the exchange codes in your translation table. Remember that each translation table may contain up to 120 exchange codes.

Translation table worksheet

Table ID: _____ **Area/City Code:** _____

Prefix for exchange codes in the table: _____

Prefix for exchange codes NOT in the table: _____

Exchange codes:

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

Compiling a list of required translation tables

To prepare the data for translation tables, follow these steps.

Step	Action
1	Does your system need a translation for any of the four exceptional dialing situations? • If yes, continue with this procedure. • If no, you do not need this procedure.
2	Select the area code and the two prefixes for exchange codes in, and not in, the translation table.
3	Fill in the associated exchange codes. **Note:** It is recommended that you configure a table that requires fewer exchange codes for the prefix with exchange codes *in* the table than for the prefix with exchange codes *not in* the table.
4	Repeat steps 2 and 3 if there are more exceptional dialing cases requiring a table.

Local dialing to a different area/city code (area/city code required)

Introduction

The area/city code of the dialed DN is different from your local system's area/city code, but no long distance charges apply and a local dialing prefix is required *instead* of a long distance prefix. The area/city code is required as part of the dialable DN.

Scenario

This scenario may occur in larger metropolitan areas that are serviced by a number of area codes. For instance, a large city may have two or three area/city codes (like 416 and 905) to cover the entire metropolitan area.

When a call is placed from the 416 area/city code to some exchange codes in the 905 area/city code, the call may be local. However, for other exchanges, the call may be considered long distance. For those exchanges that are considered local, the long distance prefix must not be inserted in the dialed DN.

In this scenario, the area/city code of the dialed DN is different than your local system's area/city code. However, the local dialing prefix must be included in the dialed number, *not* the long distance prefix. (Charges do not apply to certain calls to the destination area/city code, and the long distance dialing prefix need not be used.) The area/city code *must* be part of the dialable DN.

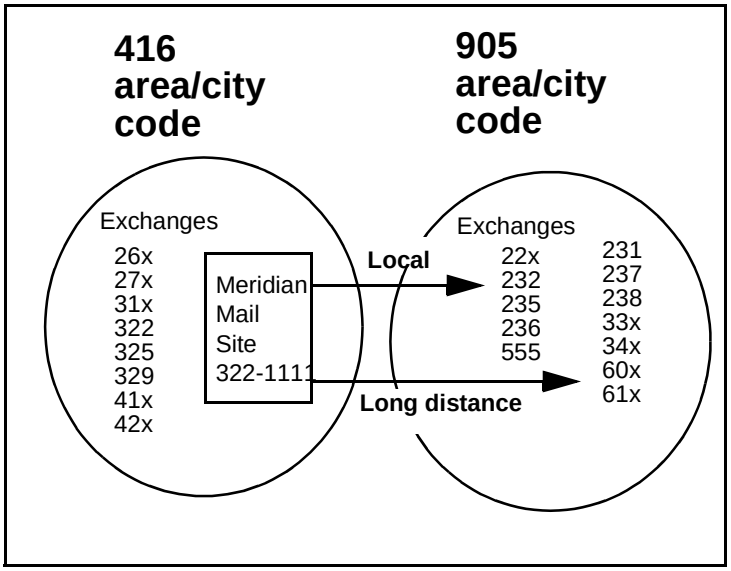
A translation table is required for each area/city code that has *both* local and long distance exchanges, and is dialed from your local system.

Area/city code required for local call

As you can see in the following diagram, in the 905 area code, the exchange codes 22x (which means from 220 to 229), 232, 235, 236, and 555 are local from the 416 area/city code.

Exchanges 231, 237, 238, 33x, 34x, 60x, 61x are all long distance from the 416 area/city code

.



Example

Your Meridian Mail system is located in area/city code 416. The network dialing prefix is 9 and the long distance prefix is 91. A caller phones your system and requests a fax item. Your Fax on Demand service is configured for callback delivery, so the caller is prompted for a callback number in national format. The caller enters 1-905-555-2121 (the 1 is the country code).

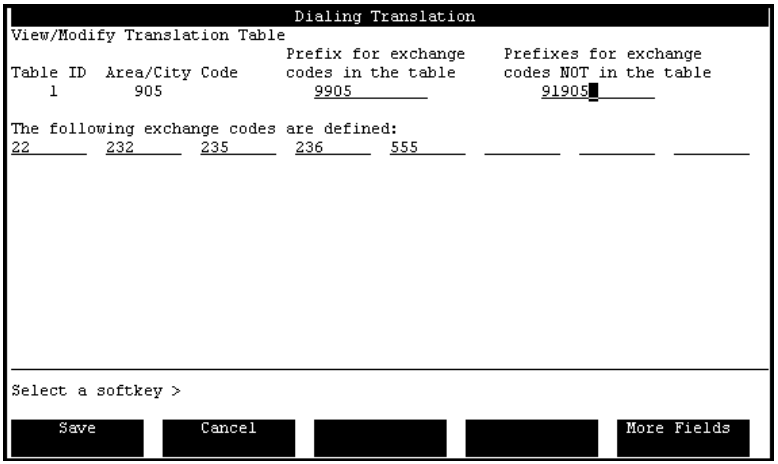
If you look at the exchange code diagram above, you will notice that calls to the 555 exchange are considered local. The dialable DN is therefore 9-905-555-2121, and not 91-905-555-2121.

Translation table setup (version 1)

The screen example on page 18-54 shows the translation table that you would have to create to handle the above scenario. This screen example assumes that the local dialing prefix is 9 and that the long distance dialing prefix is 91.

Screen (version 1)

The following screen illustrates the version 1 translation table.



Logic of version 1

This example selects those exchange codes in area/city code 905 that require only a local call to area/city code 416. The example shows that the exchange codes (22x, 232, 235, 236, and 555) are local and, therefore, they are assigned the Prefix for exchange codes in the table.

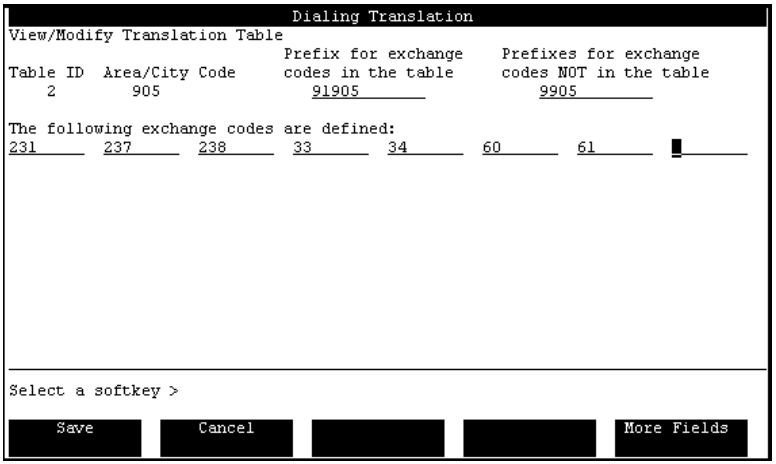
Any other exchange code will be considered long distance by consequence and will be assigned the long distance prefix (91-905), which is defined in the Prefix for exchange codes *not* in the table field.

Translation table setup (version 2)

You could also define the translation in the inverse manner from version 1. That is, you could define the exchange codes that require the long distance prefix, while the remaining exchange codes would be assigned the local prefix by default.

Screen (version 2)

The following screen illustrates the version 2 translation table.



Logic of version 2

The exchange codes that are long distance within the 905 area/city code are explicitly defined in the table instead of the local codes. (Note that the two prefixes for exchange codes in the table and exchange codes *not* in the table fields are reversed from version 1).

Hint for planning translation tables

The way in which you define the table will depend on how many exchange codes within the area/city code are considered local and how many are considered long distance. If, for example, 100 exchange codes in the 905 area/city code are long distance and ten are local, the version 1 translation table would be easier to create since you would have to define only ten codes. However, if there were more local exchange codes than long distance codes, you would create a table similar to that in version 2.

Local dialing to a different area/city code (no area/city code required)

Introduction

This scenario is almost identical to the first scenario because there is local dialing from one area/city code to a different area/city code. However, the difference is that no area/city code is required in the dialable DN. Using the example from page 18-52, the dialable DN would be 9-555-2121 instead of 9-905-555-2121.

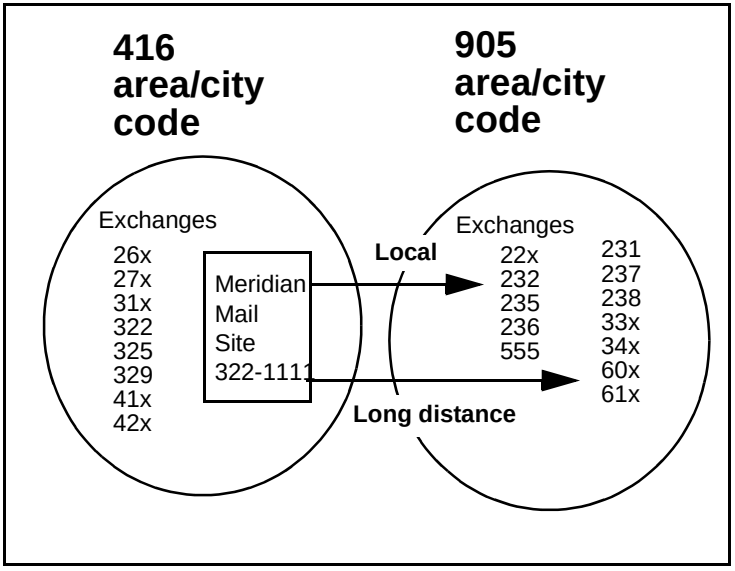
Scenario

This situation may occur if, for example, a metropolitan area is in the process of adopting a new area code in which certain exchanges will be considered local (as described in the previous example).

Therefore, in the exchange code diagram that follows, the first column of exchange codes in the 905 area code are local if dialed from the 416 area code. In order to make the transition easier for people in the area, the service provider will allow calls to the local exchanges in the 905 area code to be placed without the area/city code since this is what people are accustomed to dialing. However, after a certain specified date (when the phone company ends the transition period), the new area code will have to be entered and the translation table prefixes updated (to those in the previous example).

Area/city code not required for local call

This diagram shows the same relationship between 416 and 905 area/city codes as in the previous example except that this time an area/city code is not required to make a local or a long distance call.

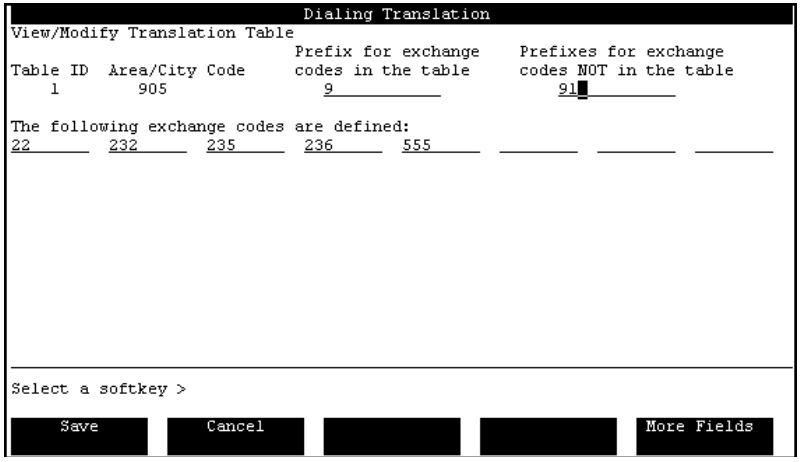


Example

If you had to create a translation table to handle the instance in the exchange code diagram above (which does not require area/city codes in a dialable DN), it would look like the View/Modify Translation Table screen that follows.

Translation Table screen–different area/ city code

This example assumes that the default translation prefix for local calls is 9 and for long distance calls is 91.



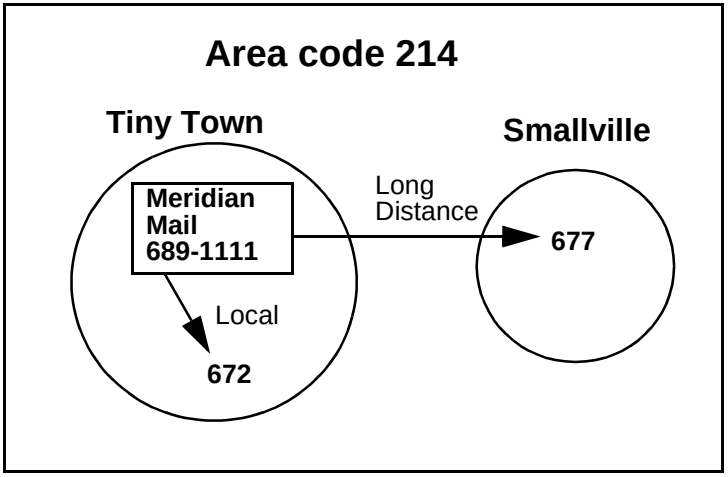
Long distance dialing to the same area/city code (area/city code required)

Introduction

This scenario describes toll call (long distance) dialing within the same area/city code. Calls involve the long distance dialing prefix even though both the calling party and the called party are under the same area code. In this scenario, the area/city code is also required as part of the dialable DN.

Scenario

This sort of dialing scenario may occur when a number of smaller rural areas or towns share an area/city code, yet calls from one town to another are considered long distance.



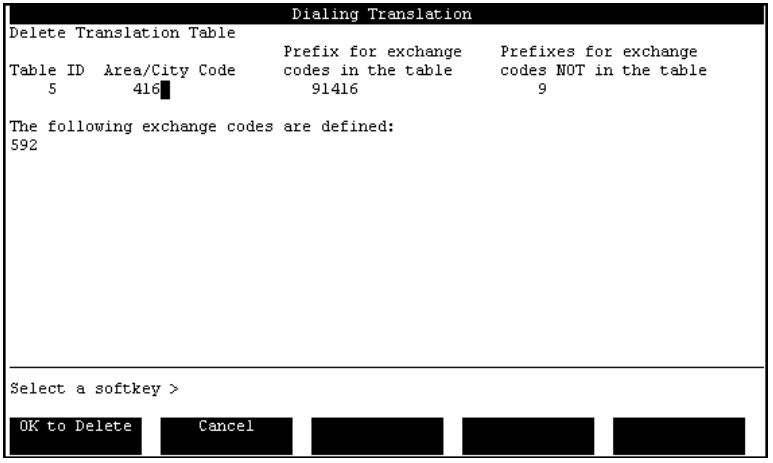
Example

A caller from Smallville calls into the Meridian Mail system located in Tiny Town and requests that a fax be delivered to DN 214-677-1133. Exchange 677 is in the 214 area code, however, so this is considered long distance because it is in a different town.

Meridian Mail must convert this DN to the dialable DN 91-214-677-1133, where 91 is the long distance dialing prefix.

Translation table

The following translation table illustrates long distance dialing to the same area/city code where the area/city code is not required to make a dialable DN.



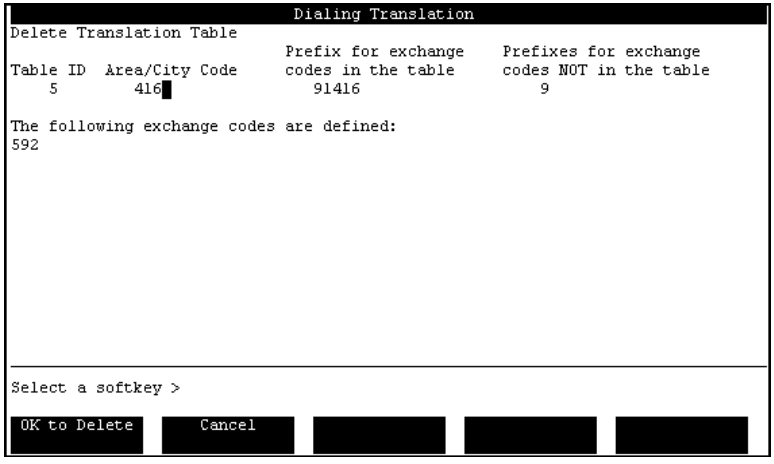
Long distance dialing to the same area/city code (area/city code not required)

Introduction

This scenario is almost identical to the preceding scenario because there is long distance dialing from one area/city code to the same area/city code. The only difference is that no area/city code is required in the dialable DN. Using the previous example, the dialable DN in this case would be 91-677-1133 instead of 91-214-677-1133.

Translation table

The following translation table illustrates long distance dialing to the same area/city code where the area/city code is not required to make a dialable DN.



The View/Modify Translation Table screen

Introduction

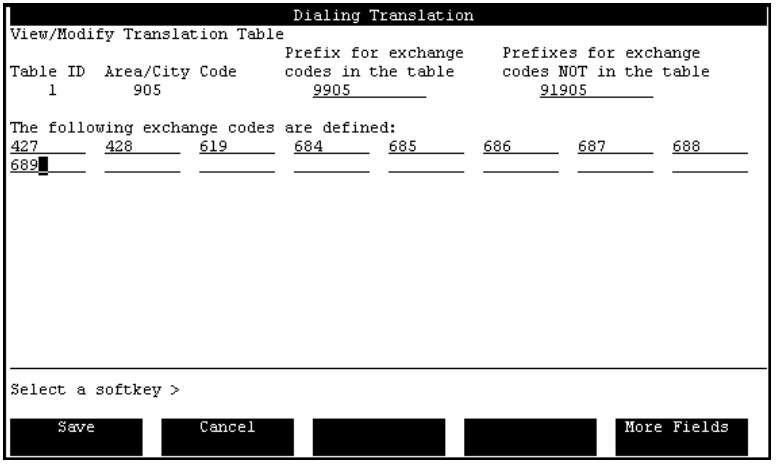
A translation table is defined on the View/Modify Translation Table screen. This subsection explains this screen and the contents of each field in the screen.

How to access the screen

See “Configuring translation tables” on page 18-64.

View/Modify Translation Table screen

The following is an example of the View/Modify Translation Table screen.



Field descriptions

The following table describes the fields in the View/Modify Translation Table screen.

Table ID	
Description	This field contains the number of the translation table.
Field status	Read-only. There are 15 tables, numbered 1-15. This is the ID of the selected table. This field cannot be changed. (Once the table is deleted, the table ID can be reused.)

Area/City Code	
Description	This field contains the area/city code of the translation table. A translation table is defined for an area/city code.
Valid characters	0-9
Valid length	1-8 characters

Prefix for exchange codes in the table	
Description	This field contains the prefix used for dialing telephone numbers in the area/city of this table, whose exchange codes are defined in the translation table.
Valid characters	0-9, * (where * means pause)
Valid length	0-12 characters

Prefixes for exchange codes NOT in the table	
Description	This field contains the prefix used for dialing telephone numbers in the area/city of this table and whose exchange codes are *not* defined in the translation table. If more than one table is defined for one area/city code, this field is enforced to be the same in every table (so that there is only one set of exchange codes *not* in any table).
Valid characters	0-9, * (where * means pause)
Valid length	0-12 characters

The following exchange codes are defined:	
Description	These fields contain the exchange codes defined in the translation table. Up to 120 exchange codes may be defined for one table. (To display more empty rows of exchange codes, press the [More Fields] softkey.)
Valid length	0-8 characters If the length of a given exchange code is 0, then that field is empty.

Configuring translation tables

Administration level

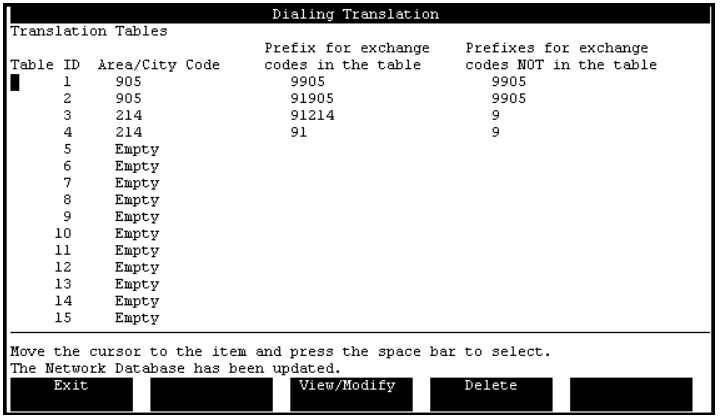
You can configure translation tables from the System Administration level only.

Procedure

To configure a translation table, follow these steps.

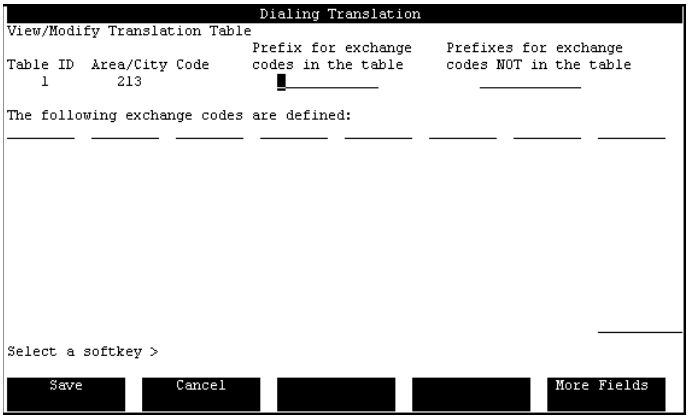
Starting Point: The Main Menu

Step	Action
1	Choose General Administration.
2	Choose Dialing Translation.
3	Choose Translation Tables. **Result:** The Translation Tables screen appears listing the existing and empty tables.



4	If you want to add a new table, move the cursor to an empty table. To modify an existing table, move the cursor to that table.
5	Press the <Space Bar> to select it.

Step	Action
6	Press the [View/Modify] softkey. **Result:** You are prompted for an area/city code.



7	Enter the area/city code for the translation table that you want to create and press <Return>. **Result:** The View/Modify Translation Table screen is displayed.
8	Specify the prefix for the exchange codes that are defined in the table. This prefix is applied to DNs entered by callers/ users in order to generate the appropriate dialable DN.
9	Specify the prefix for exchange codes that are *not* defined in the table. This prefix is applied to DNs entered by callers/ users in order to generate the appropriate dialable DN.

Step	Action
10	Enter the appropriate exchange codes. To display more empty fields, press the [More Fields] softkey. Up to 120 exchange codes can be defined for a table. **Note:** All entries will be validated to avoid duplication.
11	Do you want to save the screen? • If yes, press the [Save] softkey to save the table. **Result:** The updated Translation Tables screen is displayed. **Note:** If you run out of exchange code fields for an area/city code, create another table for that area/city code. Return to step 4. The values you enter in the Area/City Code and the Prefix for exchange codes *not* in the table fields of the second table must match those of the first table. • If no, press the [Cancel] softkey.

Deleting translation tables

Introduction

You can use the following procedure if you want to remove a translation table in its entirety.

Administration level

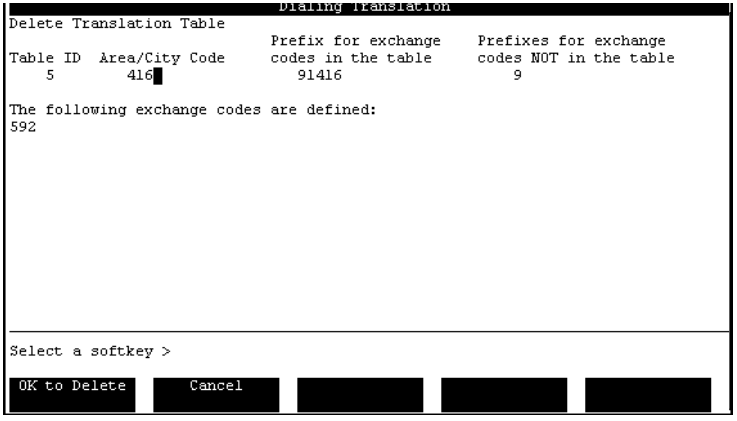
You can delete translation tables from the System Administration level only.

Procedure

To delete the data from a translation table, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose General Administration.
2	Choose Dialing Translation.
3	Choose Translation Tables.
4	Move the cursor to the (non-empty) table that you want to delete.
5	Press <Space Bar> to select it.
6	Press the [Delete] softkey. **Result:** The Delete Translation Table screen is displayed. All fields in this screen are read-only.



7	Do you want to delete the table? • If yes, press the [OK to Delete] softkey. • If no, press the [Cancel] softkey.

Section E: Sample datafills

In this section

Overview 18-70
Datafill for countries without area/city codes 18-71
Datafill for a case where the switch handles dialing translation 18-72

Overview

Introduction

This section illustrates two special cases for dialing translation which require a slightly different setup.

The two cases are

- countries without area/city codes in their dialing plans
- the switch is already handling the dialing translations

Datafill for countries without area/city codes

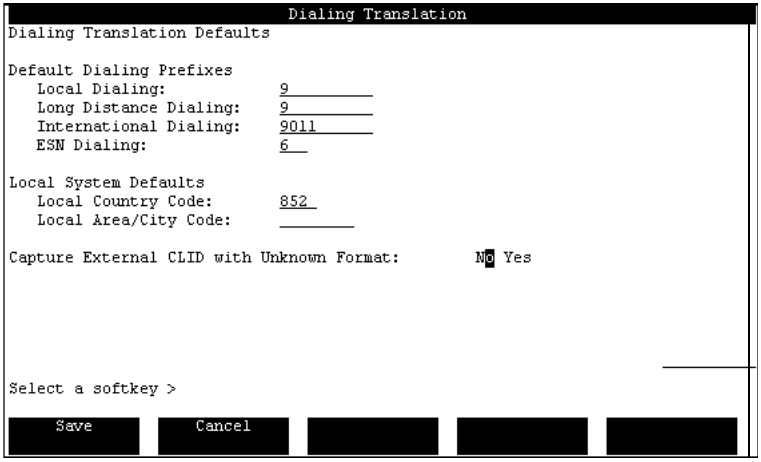
Introduction

Some countries, such as Costa Rica, do not require area/city codes for national calls in their dialing plans.

For example, the following Dialing Translation Defaults screen leaves the area/city code field blank. The other field as defined as usual.

No area/city codes screen

The following shows an example of the Dialing Translation Defaults screen defined for a location without an area/city code.



Description

When the Local Area/City Code is not entered, the system will treat *all* numbers undergoing translations as having no area/city code.

This eliminates the difference between local and long distance calls, and all national numbers will be treated in the same fashion as local numbers.

Datafill for a case where the switch handles dialing translation

Introduction

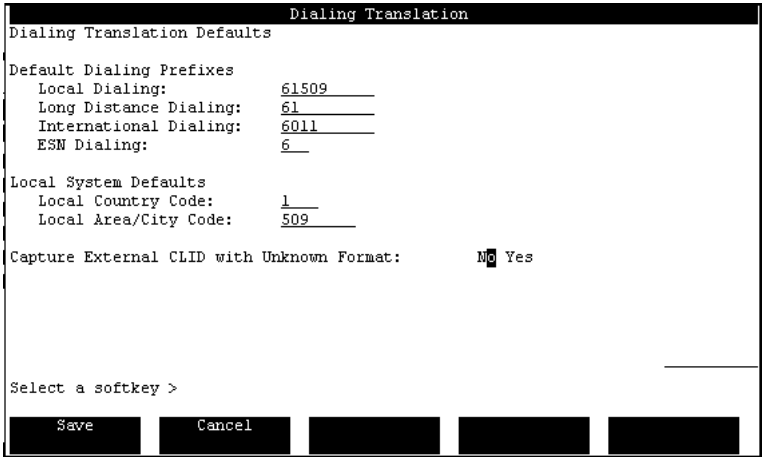
In the case where the switch is already set up and used to handle dialing translations, you may choose to *bypass* the definition of any translation tables on Meridian Mail.

In order to allow the switch to take over dialing translations, all calls must be handled by the switch.

On the M1, this can be accomplished using ESN. To implement this, all numbers dialed by the Meridian Mail must be in the same format (for example, 6-1-area/city code - local number). The switch will use its ESN software to correctly dial and route the call.

Defaults screen for switch handling translation

The following shows an example of the Dialing Translation Defaults screen with fields set so that the number passed to the switch by Meridian Mail is always in the same format so that on-switch dialing translations are used.



Scenario: International number

Company X publishes a Fax On Demand number set up for international callback for callers outside of North America. A caller from England enters the number of her fax machine as 44-628-812810 in response to the prompt “Please enter the fax

number, including country code and area or city code, followed by number sign."

The system translates the number according to the defaults in the example screen:

- The service is set up for international callback and, therefore, the system performs an international number translation on the entered number. First the system checks for the local country code (in this case, 1) at the start of the number. However, the callers country code is different.
- The caller's country code is 44 and the city code is 628, so the system attaches 6011 to create the number 6011-44-628-812810.

Scenario: Local number

The new External CLID feature has been installed on the system and allows the system to recognize the type of a number based on the information received from the switch.

An external caller leaves a message in the Meridian Mail user's mailbox. The CLID received is 795 9851, and the switch indicates that this is a local subscriber number.

To reply to this number, the number must be translated by the system as follows:

- Since this is a local subscriber number, the system knows that the number should be dialed for a local call. The system adds the local dialing prefix to the beginning of the number.
- The final number is 6 1 509 795 9851, where 6 1 509 is the added prefix.

Section F: Troubleshooting dialing translations

In this section

Overview	18-76
Diagnosing and tracing problems in a dialing translation	18-77

Overview

Introduction

This section provides you with a procedure to diagnose problems with dialing translations. It should be used in conjunction with the NTP of the feature (like the *Fax on Demand Application Guide* [NTP 555-7001-327] or *AMIS Networking Installation and Administration Guide* [NTP 555-7001-242] that uses dialing translations).

Diagnosing and tracing problems in a dialing translation

Introduction

Dialing translation problems show up as an inability to reach a number specified in the AMIS, External CLID, or Fax on Demand services. Diagnosis of such problems is best accomplished by collecting all setup information and then following the flowcharts of the translation process to determine the translated number.

Administration level

Dialing translation screens are accessed from the System Administration level only.

Procedure

To troubleshoot the translation process, follow these steps.

Step	Action
1	Collect all relevant information. **Note:** This includes the dialing translation defaults and translation table settings.

IF the problem occurred in	THEN go to
Fax on Demand	the Fax on Demand VSDN definition and session profile.
AMIS	local AMIS VSDN definition.
Virtual Node AMIS	local AMIS VSDN definition and the VSDN definition of the Virtual Node AMIS remote site.
External CLID	the External CLID (the caller's number) to which the user listened or to which the user tried to send a message.

2 Is the translated number already dialable?

- If yes, go to step 5.
- If no, the dialing translation setup is likely incorrect. Continue with the following steps.

Step	Action
3	Determine the translated dialable number that was found to be invalid.

IF the invalid number used	THEN
Fax on Demand	the Fax Audit Trail will contain the translated DN that the system is attempting to dial. For more information about the Fax Audit Trail, see Chapter 34, “Audit Trail reports” under Section C: Fax Audit Trail reports.
AMIS	SEER 4211 is generated. (The SEER text is “The number XXXXXXX cannot be reached,” where XXXXXXX is the translated number).
External CLID	ask the user for the number that is announced by Meridian Mail when listening to the message from which the error was reported.

4	Pick a particular scenario that is causing problems and walk through the translation process flowcharts from page 18-23 to 18-26 to determine the translated number. This method will help you determine if the problem is caused by dialing translations.

Step	Action
5	If the translated number is dialable on the system, then the problem may not be related to dialing translations. In this case, the problem is likely to be one of the following: • The fax callback number, AMIS number, or External CLID number is restricted in the Meridian Mail restriction/ permission lists and cannot be dialed. • For External CLID, the number that is passed from the switch to Meridian Mail may be incorrect. Use the Session Trace feature from the Tools level to determine the number and call type that was received from the switch when the external caller left the user a message in the user's mailbox. • For External CLID, refer to *System Administration Tools* (NTP 555-7001-305.) • For Fax on Demand, check the session profile and ensure that it is set up correctly. • For AMIS, check the class of service to which the user belongs and ensure that it allows the user to send or receive Open Network (AMIS) messages. • The area/city code of the callback number or AMIS number may be restricted on the switch. Check LD 90 in the Meridian 1. • Alternatively, the entire number may be restricted because it is considered a "special number" (also check LD 90 in the Meridian 1). • The agent is restricted in the switch. Check NCOS and FCAS in LD 87.